Global Information Assurance Certification Paper

Designing a Secure Windows

2000 Infrastructure

David Malcom

GCWN Practical Assignment

Version 3.1

Option 1 – Design a Secure
Windows 2000 Infrastructure

Table of Contents

Introduction

GIAC Enterprises is an Application Service Provider company specializing in the primary and secondary education market. GIAC Enterprises consists of a corporate headquarters in Lincoln, Nebraska; a corporate office in Ogallala, Nebraska and 10 remote sites located within various Educational Service Units throughout the state.

The nature of this document is to explain the security considerations GIAC Enterprises has taken into account and the lengths to which they've gone to protect customer information. It will cover in detail the design for a secure Windows 2000 Active Directory infrastructure for GIAC Enterprises. It will be comprised of four main sections.

GIAC Enterprises Overview - It is important to know a little of the history behind GIAC Enterprises to fully understand the design considerations and security concerns presented here.

Network Design and Diagram - A graphical representation of GIAC's infrastructure including internal networks and production networks followed by descriptions and explanations.

Active Directory Design and Diagram - This is a visual representation of GIAC's corporate Active Directory layout organized by internal departments. In addition, this layout will be dissected and explained in detail. Also included is a design and breakdown of a typical Active Directory domain housed at a remote site.

Group Policy and Security - The heart of GIAC's security implementation. This section details specific Group Policy settings that have been implemented to guarantee a high level of security on customer accessed servers. GIAC's internal implementation of Group Policies is detailed here. Additional Security implementations outside of Group Policies are discussed at the end of this section.

GIAC Enterprises Overview

GIAC Enterprises was founded in 1998 with a corporate headquarters in Lincoln. The idea behind the company was to provide terminal based Application Hosting for schools throughout the Midwest. GIAC is currently concentrating on the Nebraska market to gain a strong base of support for the product. Once that happens GIAC will begin marketing to schools outside of Nebraska.

With a strong knowledge of public school network design and the infrastructure supporting them, GIAC was able to create a cost-effective way for schools to keep up on cutting edge software and technology.
The idea is based around utilizing the existing networks and infrastructure that schools generally purchase/lease from Educational Service Units. There are nineteen ESUs throughout Nebraska that support between twenty and fifty school districts each. Schools generally obtain their internet and e-mail access from the ESU through leased lines connecting them directly to the ESU.

GIAC has negotiated leased space within the ESUs to serve as their remote sites. From this location, GIAC can implement Citrix servers that host applications for the schools to launch remotely. GIAC has worked with numerous software companies to be able to provide a list of supported applications for all aspects of the educational environment. Schools are able to choose from this list what applications they would like to have made available to their student body and faculty. Additionally GIAC has made available a test environment in which applications a school desires, but are not on the list, can be loaded and ran through compatibility testing. This service is available at an additional cost along with some premium programs that require extensive system resources to run. Some currently available applications include:

- The Microsoft Office suite
- Microsoft Internet Explorer
- Microsoft FrontPage
- Macromedia Flash MX
- Orchard Software – Includes modules for Science, Mathematics, Reading, Language Arts, Phonics, Social Studies, and Vocabulary Building
- Transparent Language Learning software
- Adobe Photoshop
- Adobe PageMaker
- AutoDesk AutoCAD
- Mavis Beacon Typing Skills
- Peachtree Accounting software
- GradeBook Power

These benefits allow customers to leave the hassle of software installations and updates; not to mention licensing headaches, to GIAC. They are also able to drastically cut their hardware costs of server and workstation replacements since all of GIAC applications will run on a simple thin-client or low-end workstation. GIAC now has over 100 clients that have seen the value of our flat-fee based Application Hosting.

The corporate headquarters in Lincoln consists of the following departments:

- Corporate Accounting and Finance
- Human Resources
- Sales

- Corporate Communications and Marketing
- Customer Support
- Data Communications
- Internal Support

The corporate office in Ogallala was added in 2001 to meet the ever growing needs for compatibility testing and a strong desire to make the published applications available through a standard internet connection. It was also at this time that GIAC added a third corporate branch: Research and Development. Departments in Ogallala include:

- E-Business
- Development
- Sales
- Customer Support

The ten remote production sites provide a location from which GIAC's engineers can troubleshoot problems and perform infrastructure maintenance, but no employees are permanently based from them. GIAC has production sites in the following Educational Service Units:

- ESU 2 – Fremont Nebraska
- ESU 5 – Beatrice Nebraska
- ESU 6 – Milford Nebraska
- ESU 9 – Hastings Nebraska
- ESU 10 – Kearney Nebraska
- ESU 11 – Holdrege Nebraska
- ESU 13 – Scottsbluff Nebraska
- ESU 14 – Sidney Nebraska
- ESU 15 – Trenton Nebraska
- ESU 16 – North Platte Nebraska

Network Design and Diagram

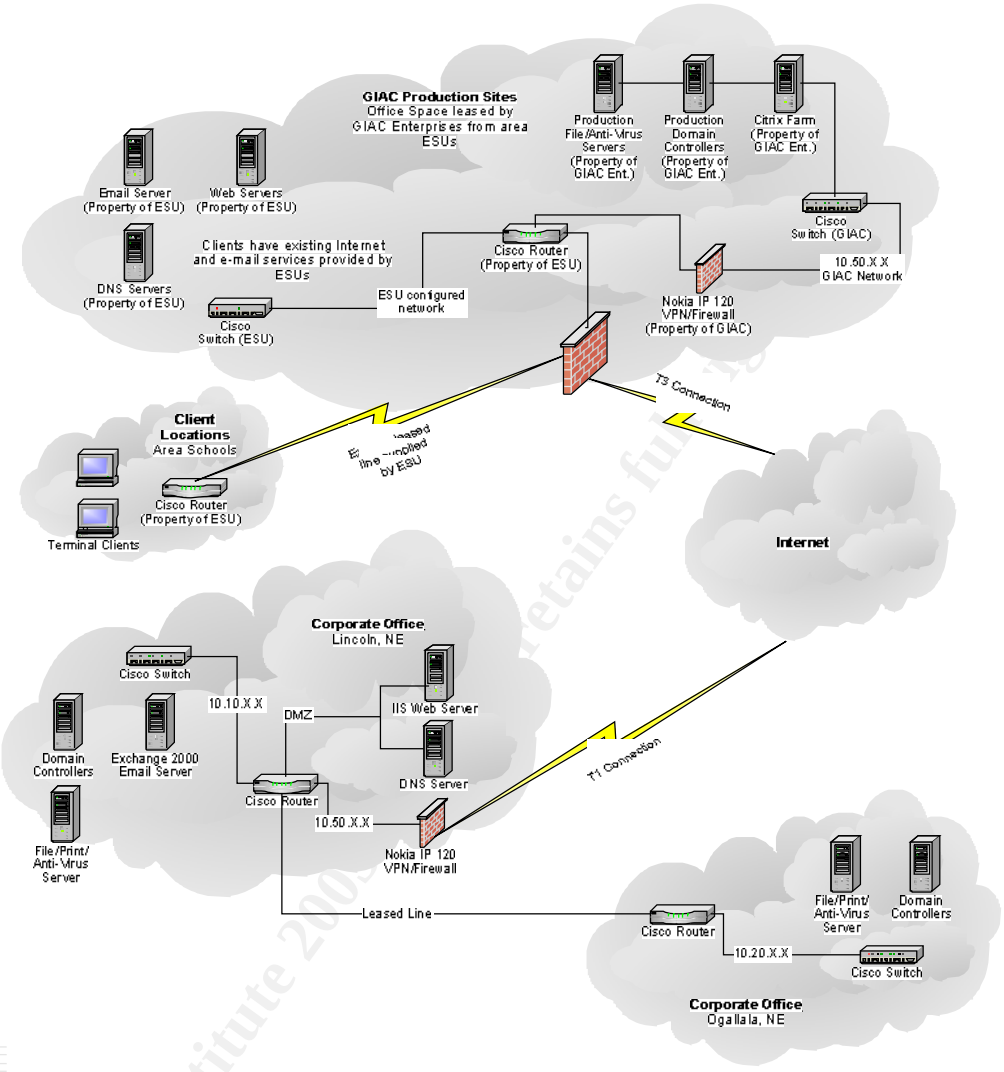


Figure 1 - Network Diagram

GIAC's global networks consist of 2 corporate sites and 10 remote production sites. GIAC employees residing in the corporate offices maintain the ability to service and control the remote site locations by way of a T1 connection to the internet and VPN tunnels to each site. Due to security concerns no traffic that is not encrypted is allowed to travel to the production segments. To accomplish this GIAC utilizes Nokia IP120 firewall/VPN devices.

Although the production domains are fully owned and maintained by GIAC, they are separate from the corporate domain with no trusts established. All administration of the remote sites is done through the 10.50.X.X network. GIAC employees that are in charge of monitoring and administering remote sites, do so through Terminal Services which has been installed on all productions servers.

The Remote Desktop Protocol (RDP) that controls Terminal Services and normally listens on port 3389 has been changed to port 9797. All access to port 9797 is logged and monitored. Also, within Terminal Services Configuration, permissions to use the RDP protocol have been limited to the Domain Admins group of the production domains.

Customer access to production domains is accomplished through the Citrix ICA service only. Access to this service, and the applications that can be launched within it have been limited through Citrix's Connection Configuration application.

GIAC prevents unauthorized connections to the internal network from the production networks by way of router Access Control Lists. If communication was not initiated by a user in the internal network, it is not allowed to travel back to the internal network.

Server Base Configurations

- Windows 2000 installations are customized and unless necessary, all IIS services and SNMP management are removed.
- All servers are configured with a RAID 5 NTFS disk system to accommodate performance and redundancy issues.
- To maintain consistency only Dell servers with Windows 2000, Service Pack 3 are used.
- All servers run the latest version of Internet Explorer with all applicable security updates.
- Hotfixes are applied to servers during non-business hours with Update Expert software from St. Bernard.
- All servers are protected by UPS battery backup. All hardware is supported 24 X 7 by the vendor.
- Non-critical hardware replacements are to take place during scheduled downtimes.
- Production File Servers are configured with external disk arrays. This provides the best environment for growth on an as-needed basis.
- File Servers at both the corporate offices and the remote sites are in charge of backups and anti-virus software for all servers. Backup Exec from Veritas is used for backups. Each server has an agent installed and is backed up over the network. Backups are performed on a nightly basis and copies are taken off-site weekly to a secure location. Norton AntiVirus Corporate Edition is used at all locations. Updates for virus signatures are checked for on an hourly basis with updates being pushed to clients as soon as they are downloaded by the Enterprise AV servers.
- Unnecessary services on all servers are set to either disabled or manual. These include:
    1. DHCP Client – All servers had static IP address, so this is not needed

2. IIS Admin Service - This service runs only on the external IIS Server
3. Browser Service - Only turned off on the external IIS and DNS servers
4. Indexing Service – Not needed on any servers
5. Clipbook Service – Not needed on any servers
6. DFS - Turned off on the external IIS, DNS and production Metaframe servers.
7. Fax Service – This service is not needed on any servers
8. Intersite Messaging - This service runs on domain controllers only and is used for Active Direction replication
9. Kerberos Key Distribution Center – Runs on all domain controllers and grants tickets for Kerberos authentication
10. Server – This is disabled on the external IIS and DNS servers
11. Workstation – This is also disabled on the external IIS and DNS servers
12. TCP/IP NetBIOS Helper Service – This service is disabled. It allows backward compatibility authentication with NTLM which is not needed at GIAC
13. Messenger – This service is needed to transmit messages on the Metaframe servers. It is disabled on all others.
14. NT LM Security Support Provider
15. Removable Storage – Used for removable disks and tape libraries. These functions are controlled by Backup Exec.
16. Remote Access Auto Connection Manager – Used for dial-up environments
17. Remote Access Connection Manager – No servers run RRAS
18. Remote Procedure Call – Runs only on domain controllers
19. Internet Connection Sharing – disabled on all servers
20. Print Spooler – Runs only on the internal File/Print servers and on production Metaframe servers
21. Telephony – disabled on all servers
22. Telnet – No telnet sessions are allowed to servers
23. Utility Manager – Not needed on any servers
24. Windows Management Instrumentation – This is used by NetIQ on most servers, but does not run on external DNS or IIS servers

Server Roles and Specifications

Both Corporate Locations

- Active Directory domain controller – These servers provide all authentications for employees to the corporate domain (giac.corp). They run DNS in Active Directory integrated mode and DNS is set to allow for dynamic updates from secure sources only. The “Secure cache against pollution” option has been enabled on all DNS servers to prevent DNS poisoning. Also DNS zone transfers have been disabled. Group Policies

are maintained on these servers providing logon scripts and domain-wide security implementations

- File/Print/Anti-Virus server – These servers are configured with 140 GB of drive space each. Each server houses files for their respective site and corporate shares are created for each department within GIAC. All security on these shares is NTFS based and access is controlled on a group basis by department. Individual user home directories are also on these servers with a 1 GB limit per user managed by Quota Advisor software from W. Quinn Associates.

Lincoln Office only

- Email server – Runs Exchange 2000 with Service Pack 3 and the Exchange 2000 post SP3 rollup. The Microsoft Baseline Security Analyzer has also been run on this server to check for Exchange security vulnerabilities.
- External Web Server – This server runs IIS 5.0 and is not a member of any domain. This server has had all security hotfixes applied and has also had the IIS Lockdown Tool ran against it to verify that it is running a minimal set of services. Only static HTML pages are needed so unnecessary services have been removed. These include: Internet Printing, FTP, SMTP, NNTP and Front Page Server Extensions.
- External DNS Server – This server is not a member of any domain either. Unnecessary services and dynamic updates to DNS have been disabled. Records on this DNS server are updated manually and changes are only allowed by two accounts. Log files are monitored and backed up regularly. The internal DNS servers use this server as a forwarder for internet traffic. It also houses the MX record for the Exchange server.

Remote Production Sites

- Active Directory domain controllers – There are two domain controllers per production site. These domains are completely separate from GIAC's corporate domain and also are separate from each other. Production domain names are derived from the ESU they are house in. For example GIAC's production domain in ESU 2 is named esu2.giac.prod. User accounts are created for each school and are in one of three categories: Student, Teacher, or Administration. All client accounts have the same limited rights on the domain; the difference is in the applications that are published for them. Through Group Policies, clients receive mapped drives to their home directories and public shares on GIAC's production files servers.
- File/Print/Anti-Virus server – Similar to corporate servers of the same type, these servers start with 280 GB of space but external arrays allow for up to 5 TB. Shares are created for each school with each account getting a home directory limited to 200 MB by Quota Advisor. There are also per-school group shares where all users from each group of each school can

share information. Permissions are set at the NTFS level and controlled by group.

- Application servers – Loaded with Citrix MetaFrame XPa. These servers house all applications that a school pays to run. Applications are load-balanced between servers in the Metaframe Farm to provide redundancy. Users are only allowed to run published applications in their Metaframe Session and once they close an application; their connection to the server is immediately dropped. This prevents access at the system level. These servers are rebooted on a nightly basis to alleviate the problem of memory leaks associated with a terminal environment.

Active Directory Design and Diagram

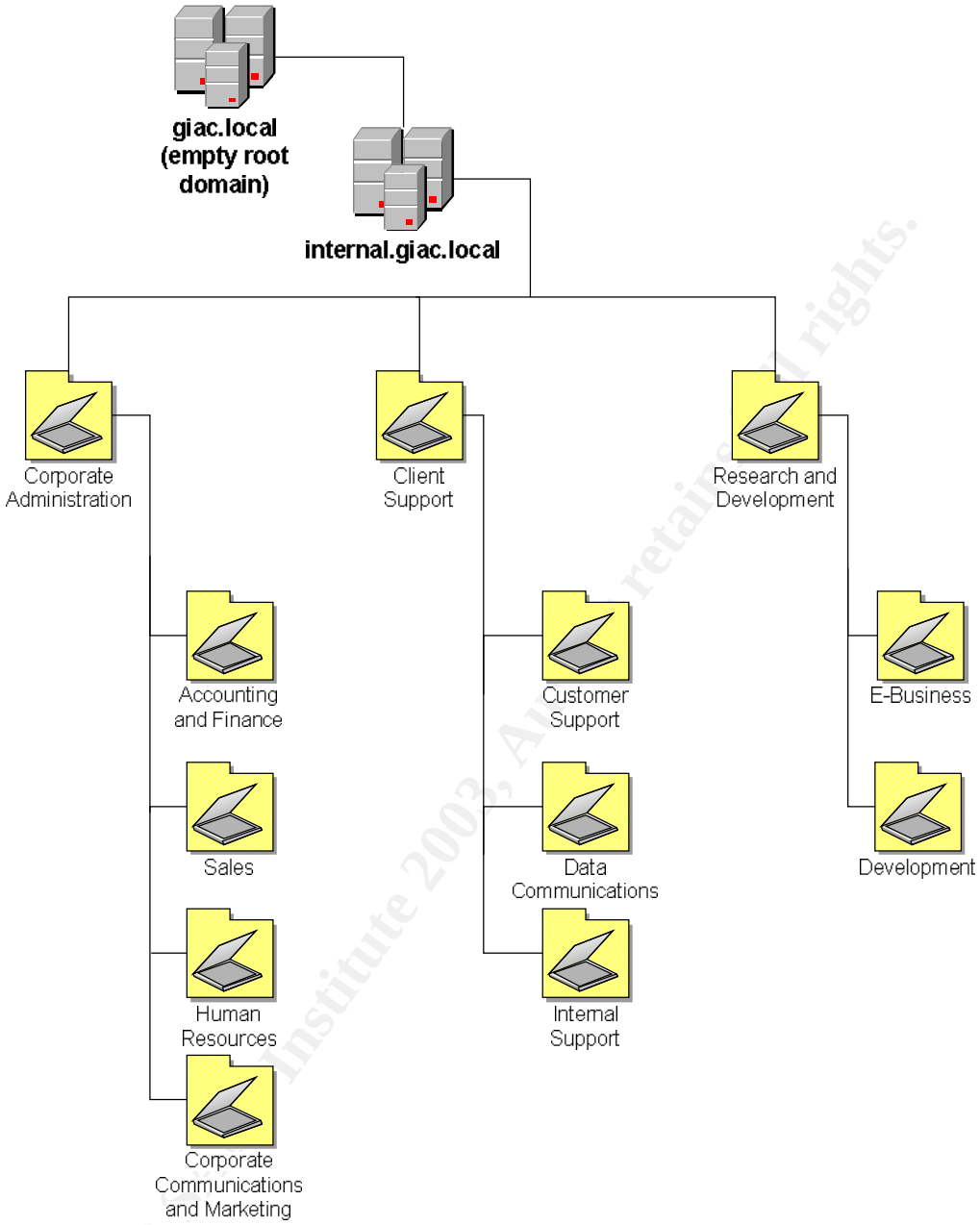


Figure 2 - Active Directory Domain and OUs

Internal AD Design

Empty Root Domain

The decision was made at GIAC to use an empty root domain when implementing Active Directory. The possibility of someday bringing the production domain and the internal domain into the same forest created enough potential issues that it was determined to be worth the cost of the extra root level domain controller. Security concerns in that environment would require an ability

to control more aspects of security than are possible at only the Organizational Unit (OU) or site level.

By using an empty root forest, GIAC is able prevent the internal domain from becoming obsolete along with allowing GIAC to potentially grant control of entire domains within the organization without compromising certain Flexible Single Master Operations Roles (FSMO) within the forest. The two Forest-wide FSMO roles are:

- Schema Master – This role is housed on the root domain controller. It controls all aspects of the Schema for the forest.
- Domain Naming Master – This role is also on the root domain controller. It will maintain consistency and prevent duplicates throughout future domains within GIAC's forest.

With an empty root domain GIAC is able to control who is a member of the Enterprise Admins groups which gives them control of the Schema Master and Domain Naming Master roles.
There are three remaining roles that exist on a per domain basis. They are:

- PDC Emulator – This role allows Windows NT BDCs to function on a mixed-mode Active Directory. GIAC is in a native-mode environment which relegates this role to re-processing failed authentication attempts to other domain controllers. GIAC's domain controller in Lincoln provides this role.
- RID Master – The RID Master assigns Relative Identifiers (which make up part of a computer's SID) to domain controllers. This role is on GIAC's Lincoln domain controller since that is where most employees reside and where most computer accounts are created.
- Infrastructure Master – This role ensures that changes to objects, such as user or group names, are replicated throughout the domain. Once again, since Lincoln's domain controller sees the majority of these changes initially, it holds the Infrastructure Master role.

All three of GIAC's internal domain controllers house a copy of the Global Catalog. Should a lot of growth occur that would justify more domain controllers; global catalog placement would need to be re-addressed and optimized. Until then, this scenario provides adequate performance with the necessary redundancy throughout the Active Directory.

Domain Suffix
The domain suffix of .local was chosen because GIAC has registered giac.com for its external web presence and none of GIAC's internal servers or computers will need to be accessed directly from the internet. This suffix prevents them from being referenced by a DNS server with an internet presence.

Domain Trusts
Production domains are not part of the GIAC corporate forest and there is no trust established between these sites and GIAC's internal domain. This is by design and is an important part of GIAC's security considerations. This provides the customer the assurance that only a very select number of GIAC employees will be able to access the servers that they trust with their information. It also helps prevent unauthorized access from the production sites should one of the Metaframe servers become compromised.

All GIAC employees fall into one of three main branches within GIAC. These branches are Corporate Administration, Client Support and Research and Development. Currently all of GIAC's group policies that affect computers only are applied to these three OUs. This is because any modifications that GIAC applies to workstations conveniently fall into one of these three groups. User level group policies are applied to lower level, child OUs that house only users and groups. Separating their users into these lower level OUs allows GIAC to delegate control over each group to the manager directly in charge of those groups.

The internal OUs are broken down as follows:
Corporate Administration – All computers within the Corporate Administration OU are set to install and repair a custom installation of the Norton Anti-virus client upon boot-up. This install points them to the Corporate Norton server in Lincoln for updates. The Microsoft Office suite is also deployed to them through software installation. Corporate Administration contains these lower-level OUs:

- Accounting and Finance – Users in this OU run a special logon script that maps them to a private share on Lincoln's file server. This share houses sensitive accounting information.
- Sales –In addition to standard drive mappings, these users map to a DFS share that is replicated between the Lincoln and Ogallala office. This share keeps a synchronized set of files for Sales employees to access when they travel between sites.
- Human Resources – This group has been give access to a custom MMC that allows them to edit specific details of Employee user accounts.
- Corporate Communications and Marketing – This is the only group that has Adobe Photoshop automatically installed on their workstations.

Client Support – Computers in this OU also install a Norton client that receives updates from Lincoln's Anti-Virus server. Lower-level OUs are:

- Customer Support – This group has a custom, redirected desktop that provides quick access to support tools for them to monitor production servers and troubleshoot problems.
- Data Communications – This group is mostly concerned with router and switch maintenance and needs no special OU configurations.
- Internal Support – This group is similar to Customer Support; however, their customers are GIAC employees. They are given a pre-configured

installation of PCAnywhere that is used to diagnose computer problems remotely.

Research and Development – This is GIAC's newest corporate branch. Computers in this OU run scheduled local backups to protect sensitive data. There are two lower-level OUs in Research and Development. Workstations in this OU receive Anti-Virus updates from the files server in Ogallala.

- E-Business – This group employs contractors to work on web-based services for GIAC. Because of this, these computers are locked down with Group Policies to prevent unauthorized access.
- Development – Users in this OU are given Microsoft Access as a development tool.

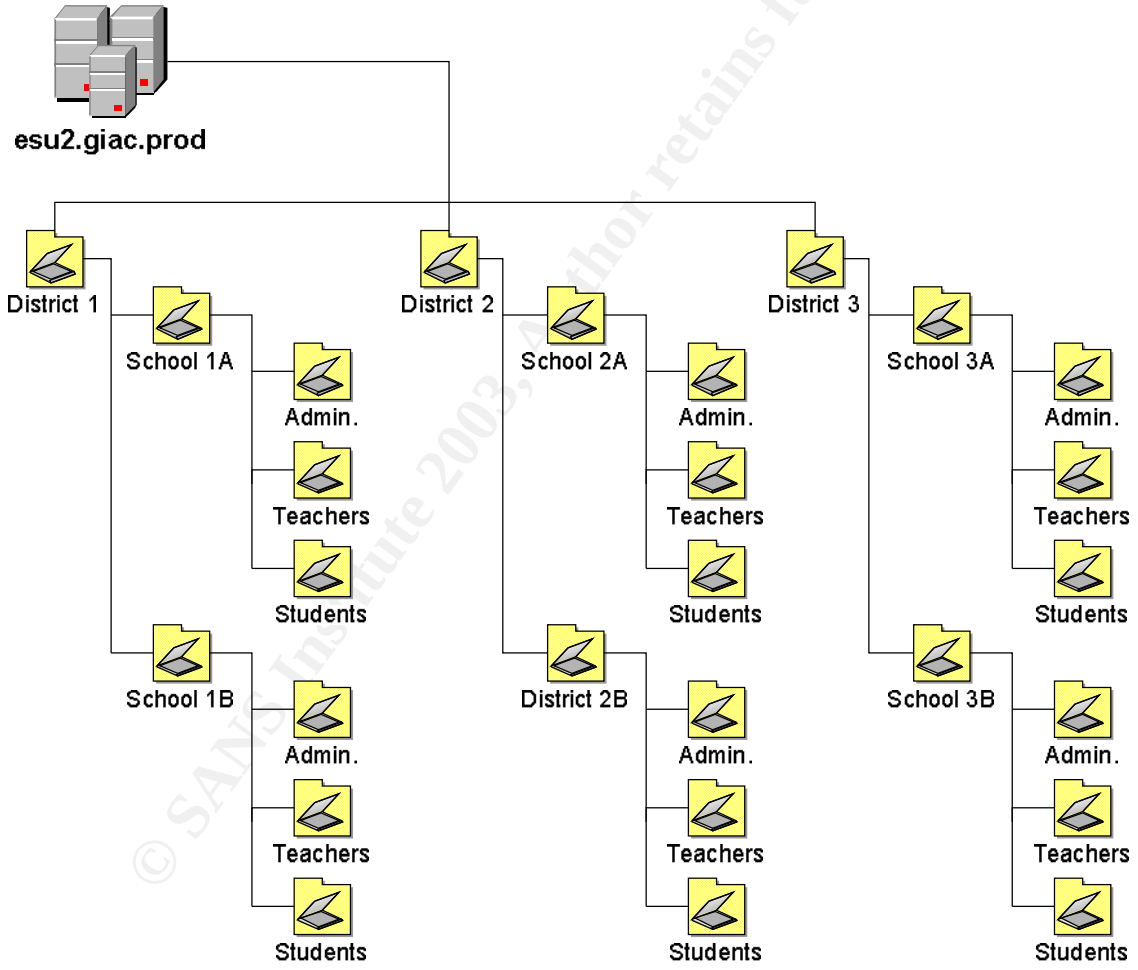


Figure 3 - Production AD Diagram

Production AD Design
All production domains follow a standard design. There are upper-level OUs created for each school district that is a member of this ESU. Under the School District level there are OUs for each participating school in this district. The lowest-level child OUs are created for the three types of clients: Administration, Teachers and Students. Since all security is the same for every client, this breakdown is mainly for ease of administration purposes. It does, however allow for delegation to certain individuals in each OU for tasks such as password resets.

For production domains, FSMO role handling is simple. There are two domain controllers for each production site. Each one houses a copy of the Global Catalog and the first server brought online maintains all FSMO roles.

Site Replication Design
Since GIAC's internal domain encompasses two physical locations that are several hundred miles apart, replication can be a bit of a problem. If all domain controllers were located in one physical office, replication would happen across a 100 MB LAN and bandwidth would not be an issue.

To provide the most cost-effective use of their T1, GIAC has created a site topology to minimize AD replication across the WAN. This topology contains two sites, one for each location, and specifies a timeframe for replication between sites and within sites. Replication between sites uses the IP transport and is set to occur once every two hours. Currently there is only one domain controller per site, but should GIAC add additional domain controllers within these sites, they will replicate with the RPC transport every hour.

Group Policy and Security

GIAC Enterprises uses Active Directory Policies to standardize security and configuration implementations. The two tools used are Security Policy templates and Group Policies.

Security Policies are used to control aspects such as:

- Password policies
- Account Lockout policies
- Kerberos policies
- Audit policies
- User Rights Assignments
- Security Options
- Event Log settings
- IPSEC policies

Group Policies control Computer based settings and User based settings. If a Group Policy is intended to configure only computer specific or user specific information, the non-intended portion can be disabled to allow for quicker

processing of the policy by clients. It is also possible to block inheritance with Group Policies to prevent the application of certain settings at specific OUs. In order to maintain a simple implementation, GIAC does not currently use this option. Group Policies control:

- Automatic software installation, repair and removal
- Logon and Logoff or Startup and Shutdown scripts
- Windows Components like Internet Explorer or NetMeeting settings
- Folder Redirection
- Lockdown of various Windows controls through Administrative Templates

Additional templates can be added to Group Policies to allow control of many other aspects of a connected computer or user.

Basic Group Policy

The Default Domain Policy for GIAC's internal domain has been modified to apply necessary security changes across the board on this domain. GIAC's security settings meet or exceed industry standards. GIAC followed guidelines set forth by the Department of Defense at http://security.isu.edu/pdf/cscst285.pdf [1]for Automatic Data Processing systems. Account Policies are as follows:

Default Domain Policy	Internal GIAC Setting
Enforce password history	12 Passwords remembered
Maximum password age	30 days
Minimum password age	5 days
Minimum password length	8 characters
Passwords must meet complexity requirements	Enabled
Store passwords using reversible encryption for all users in the domain	Disabled

Table 1 - Security Settings, Account Policies, Password Policy

By enabling Complexity Requirements, the system invokes a passfilt.dll file. This file forces a password to meet the following requirements as described on Microsoft's website[2]:

Passwords must be at least six characters long.
Passwords may not contain your user name or any part of your full name.
Passwords must contain characters from at least three of the following four classes:

Description	Examples

[1] US Department of Defense; Password Management Guideline; http://security.isu.edu/pdf/cscst285.pdf
[2] Microsoft Corporation; Microsoft Knowledge Base Article 279890; http://support.microsoft.com/default.aspx?scid=kb;en-us;279890

English upper case letters	A, B, C, ... Z
English lower case letters	a, b, c, ... z
Westernized Arabic numerals	0, 1, 2, ... 9
Non-alphanumeric ("special characters")	Punctuation marks and other symbols

Default Domain Policy	Internal GIAC Setting
Account lockout duration	0 (Accounts must be manually unlocked by an administrator)
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	1000 minutes

Table 2 - Security Settings, Account Policies, Account Lockout Policy

Audit Policies are configured to allow GIAC to record day-to-day happenings on the domain and monitor them for suspicious behavior. Audit Policies for the internal and production domains are configured identically. To collect and process the audited events, GIAC uses NetIQ software. In the production domains access to key administrative or backup accounts triggers alerts to be sent to GIAC Customer Support through NetIQ. These alerts are elevated to management if the attempts were not initiated by GIAC employees. To accommodate for the large amount of data that may be captured, GIAC has increased all event logs to 20 MB and retains historical event logs in offsite backup tapes.

Default Domain Policy	Internal GIAC Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit system events	Success, Failure

Table 3 - Security Settings, Local Policies, Audit Policy

Default Domain Policy	Internal GIAC Setting
Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Message text for users attempting to log on	(See below
Message title for users attempting to log on	(See below)
Rename administrator account	Clocktower
Rename guest account	Level1

Table 4 - Security Settings, Local Policies, Security Options

Anonymous access is used to create Null Sessions on Windows Operating Systems. Hackers can attempt to use null sessions to view SMB sessions or list users and groups of target machines. Setting additional restrictions for anonymous connections to "No access without explicit anonymous permissions" limits access of anonymous users to specific rights granted to this group.[3] GIAC is able to set this setting without adversely affecting legacy applications therefore reducing risk from anonymous connections to all domain computers. GIAC has renamed administrator and guest accounts to eliminate the risk of hackers only having to guess passwords to these accounts. Additionally all guests accounts are kept disabled.

The message text and message title options were set by GIAC as a requirement for successfully prosecuting anyone who may misuse their systems. These settings have been applied to the internal domain and all production domains. The text of this message was taken from an authorized banner of the Department of Energy at http://www.ciac.org/ciac/bulletins/j-043.shtml[4] and has been modified for GIAC as follows:

NOTICE TO USERS

This is a private computer system and is the property of GIAC Enterprises. It is for authorized use only. **Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.**

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to
authorized site, GIAC Enterprises, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign.
**By using this system, the user consents to such interception, monitoring,
recording, copying, auditing, inspection, and disclosure at the discretion of**

[3] Fossen, Jason; Windows 2000/XP Group Policy and DNS; pages 99-102; SANS Institute, 2002
[4] US Department of Energy; Computer Incident Advisory Capability; Information Bulleting – Creating Logon Banners; http://www.ciac.org/ciac/bulletins/j-043.shtml

```
authorized site or GIAC Enterprises personnel.

Unauthorized or improper use of this system may result in
administrative
disciplinary action and civil and criminal penalties. By continuing to
use
this system you indicate your awareness of and consent to these terms
and
conditions of use. LOG OFF IMMEDIATELY if you do not agree to the
conditions
stated in this warning.
```

Domain Controllers in an Active Directory domain are able to have a separate set of Security and Auditing policies set for them. For the most part, the policies that GIAC has in place for the entire domain are sufficient for Domain Controllers as well. There are a few additional settings however.

Domain Controller Policy	Internal GIAC Setting
Act as part of the operating system	Domain Admins
Add workstations to domain	Domain Admins
Backup files or directories	Domain Admins; Backup Operators
Change the system time	Domain Admins
Force shutdown from a remote system	Domain Admins
Log on locally	Domain Admins; Backup Operators
Manage auditing and security logs	Domain Admins
Restore files or directories	Domain Admins
Shut down the system	Domain Admins
Take ownership of files or other objects	Domain Admins

Table 5 - Security Settings, Local Policies, User Rights Assignment

To prevent unauthorized restores of Active Directory information, only Domain admins have been given the right to restore files or directories on domain controllers. For obvious reasons only domain admins should have the ability to shut down a domain controller remotely or otherwise.

Domain Controller Policy	Internal GIAC Setting
Do not display last user name in logon screen	Enabled
Rename administrator account	Netman
Rename guest account	Nothing

Table 6 - Security Settings, Local Policies, Security Options

Since domain admins are the only users that can sign on to the console of domain controllers it is important to not display the last user name on the logon

screen. Just as with the default domain policy, the administrator and guest accounts on the domain should be renamed. However, domain controllers have their own policy for this process to keep the accounts from being renamed to the same thing as their counterparts on all other domain members.

When it came to the production domains, GIAC had to walk a thin line between creating the most secure environment possible, and not making it too difficult for clients to use. Due to the nature of the Metaframe environment and it's naturally limited access, it was possible to lessen a few security policies without much overall affect to security. These settings are:

- Remembered passwords down from 12 to 6
- Maximum password age up from 30 to 60
- Minimum password length down from 8 to 6.

On the other hand, since the production domains have only servers, no actual workstations as members, certain policies should be more restrictive. The only access that clients of the production domains need are:

- Authentication to a domain controller
- Ability to sign-on locally to Metaframe servers and launch published applications
- Read and write access to mapped shares on file servers.

This meant that GIAC was able to implement all previously mentioned policies, except one, at the Default Domain Policy level. This setting was the "Log on Locally" setting which had to be configured for Domain Admins only at the Domain Controller level and also at the Local Security Policy level for File Servers. For Metaframe servers, this option had to include both Domain Admins and Domain users to accommodate Terminal clients.

Additional Group Policy

Group Policies are also used extensively throughout GIAC to accomplish desired results at the OU level. Settings configured at the OU level are applied in addition to settings applied at the domain level. However, if there is a conflict between settings at these levels, OU settings are more specific and override domain based settings. GIAC does not currently apply any Group Policy objects at the least restrictive level – the Site level.

There is one user-specific setting that is applied to every low-level department OU. GIAC could have applied this setting at the domain level but did not want it to be applied to accounts used for specific tasks (backups, NetIQ) and the administrator account. This setting should only be applied to actual employee accounts which made the department OU the logical place to apply it. This Group Policy Object (GPO) applies this setting to all employees:

- In Windows Settings → Scripts → Logon – A batch file that maps U: to \\linfs01\%username% or \\ogafs01\%username% depending on the

employee's location. This maps a home directory for each employee to folder on shared as their username on the file server in their location

In order to assure the quickest possible application of Group Policy Objects, GIAC makes a point to apply the smallest number of settings that are necessary. In addition if a policy is applying only Computer level settings, the User level of said policy is disabled and vise versa. This keeps the computer from having to process unnecessary settings and cuts down on sign-on time.

The three corporate branch OUs at the upper-most level of GIAC's Active Directory design process computer only portions of their Group Policy objects. The first branch is Corporate Administration (with a GPO of the same name) and applies the following settings to all computers in it:

- Software Installation – NortonLIN.msi is published to this group for installation (and repair if necessary) upon computer startup. This file is a pre-configured client installation of Norton Anti-virus pointing to Lincoln's file server as its primary parent server. This software is installed or checked before a user even gets a change to sign on. This ensures that all computers that are members of this OU have an anti-virus client with updated signature files. This GPO also automates an installation of Microsoft Office XP standard edition for these users.
- A startup script maps drive letters for two standard Corporate Administration network shares. These drives are: G: \\linfs01\corpshare and H: \\linfs01\public
- Runs a batch file that merges corpprint.reg into the registry of member computers under this registry key: MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce This key causes the computer to execute a one-time connection to shared printers specific to the Corporate Admin group. First time users are prompted to install the shared printers if they don't already exist on their local machines.

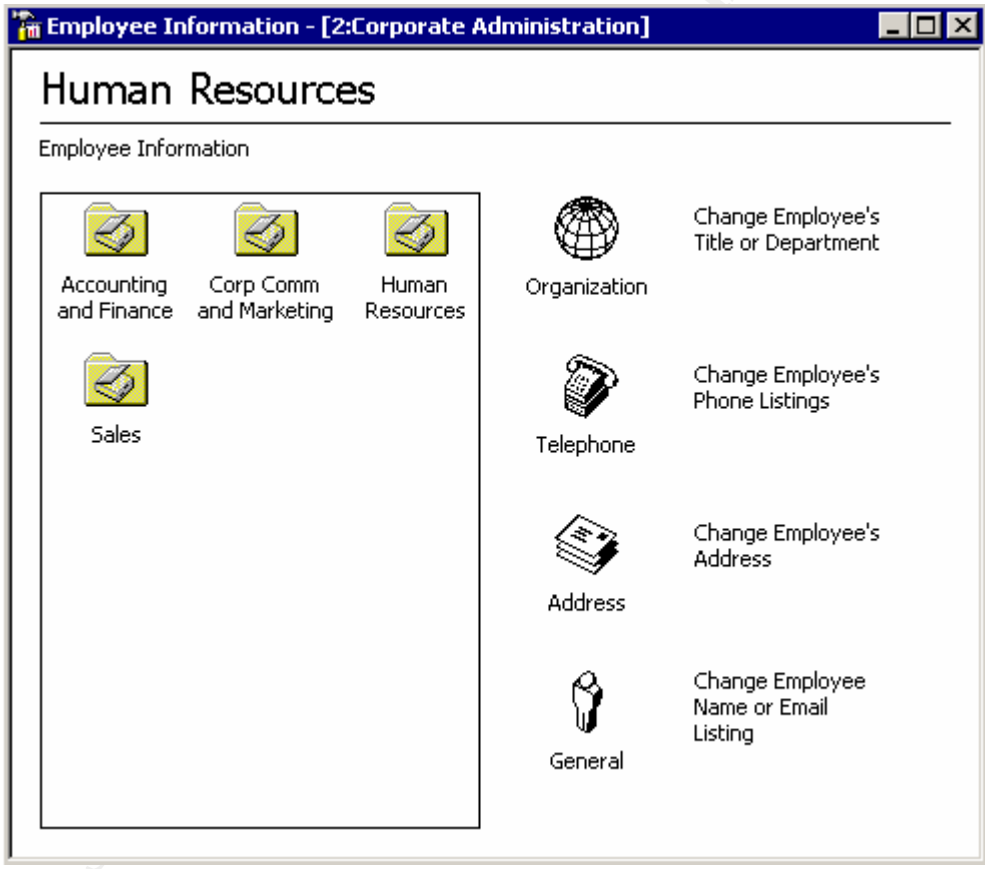
There are four user-level OUs applied within the Corporate Administration OU. The following is a list of specific user-level settings applied at each one:

- Accounting and Finance GPO – This group only maps one additional drive letter in their Group Policy object. I: \\linfs01\Accounting
- Sales GPO– Employees from this group reside in both corporate offices. This presented a minor challenge to GIAC to allow them to share current information between locations and also give them the ability to keep this information with them on their laptops when traveling. To solve this problem their Group Policy object does the following:
    1. A batch file under Windows Settings → Scripts → Logon maps a drive letter to a DFS share that is replicated between file servers in both offices. I: \\internal.giac.local\Sales.
    2. Under Windows Settings → Folder Redirection the My Documents folder for these users is mapped to the same

\\internal.giac.local\Sales. This ensures that all sales data is being backed up on the files servers and all Sales employees are working with the same information.

3. Last but not least, when a Sales employee logs off their Offline Files are forced to synchronize. This setting is under Administrative Templates → Network → Offline Files. This setting ensures that when a Sales employee goes on the road, they have a current copy of all Sales data on their laptops with them.

- Human Resources GPO– HR's GPO launches a custom mmc at sign-on for their employees. This mmc is locked down to only allow tasks that the HR group has been delegated through Active Directory. The mmc runs minimized and looks like this:



- Corporate Communications and Marketing – This GPO (named Corp Comm and Marketing) applies only one customization for Employees in this OU. Similar to the way the Norton AV client is installed, these users get a pre-configured setup of Adobe Photoshop. The .msi file that installs this software has a specified corporate license file to eliminate a need for user input upon installation.

The next corporate branch is Client Support. Only one computer-based policy in the Client Support GPO is applied to this OU. Like the Corporate Administration

branch, they run the NortonLIN.msi file for automated install of Norton Anti-virus. Network drives are also mapped to one Client Support specific network share. G: \\linfs01\csupport. Client Support contains three user-only child OUs:

- Customer Support GPO- In the same fashion that Sales has redirected My Documents folders, Customer Support has redirected Desktops. The custom desktop folder is just a DFS share that contains shortcuts that point to local hard drives for some applications and to network shares for other client-server applications. This saves Internal Support employees time by not having to install these client-server based apps on each Customer Support workstation.
- Data Communications – This group has no special GPOs currently configured for them.
- Internal Support GPO– A custom logon script with a mapped drive that contains installations to internal software is provided for Internal Support. This drive points to \\linfs01\apps. Additionally an installation of PCanywhere is automated for this group.

The last corporate branch OU is Research and Development with a GPO of the same name. Computers at this level also receive an installation of Norton Anti-virus. This installation is named NortonOGA.msi and points to \\ogafs01 as its parent AV server.
These computers also run a pre-configured session of NT backup upon log-off. Under Windows Settings → Scripts → Logoff is a batch file pointing to a shared NT backup job that begins a local backup job of these workstations to a network share on \\ogafs01\rd\backups. These workstation backups are themselves backed up by the \\ogafs01 server during its daily backup process. Employee child OUs within the Research and Development OU are:

- E-Business GPO – This OU currently contains contract-based employees of GIAC. Since there are more security concerns associated with this type of employee, these user level GPOs are locked down considerably. Settings include:
    1. Administrative Templates → Desktop → Remove Properties from the My Computer Context Menu – Enabled. Prevents right-clicking on My Computer and viewing/changing computer specs.
    2. Administrative Templates → Desktop → Hide My Network Places from Desktop – Enabled. This prevents browsing or context menu viewing of My Network Places from the Desktop
    3. Administrative Templates → Control Panel → Disable Control Panel – Enabled. This prevents all access to Control Panel Applets
    4. Administrative Templates → Network → Offline Files → Prevent use of Offline Files – Enabled. Prevents users from making network information available offline

5. Administrative Templates → System → Disable Registry Editing Tools – Enabled. This setting prevents editing the registry of the local computer.

- Development GPO – Development has an installation of Microsoft Access that is pushed to their computers. In addition there is a Development network share that is mapped through their GPO at I: \\ogafs01\Development.

Additional Group Policies that are applied to the Production domains are somewhat extensive. The upside is that besides the Security Policies configured for Default Domain, Domain Controllers, and Metaframe servers; only one GPO is needed to configure all client settings. Even though Production customers should never see a desktop of a Metaframe server, a "better safe than sorry" approach was taken in case a customer was able to access a server desktop. This GPO is set to only apply user settings since the computers that host the sessions are Metaframe servers, not client workstations. This GPO has these user settings:

- Administrative Templates → Windows Components → Internet Explorer → Internet Control Panel
  1. Disable the General Page – Enabled
  2. Disable the Security Page – Enabled
  3. Disable the Content Page – Enabled
  4. Disable the Connections Page – Enabled
  5. Disable the Programs Page – Enabled
  6. Disable the Advanced Page – Enabled
- Administrative Templates → Windows Components → Windows Explorer
  1. Enable Classic Shell – Enabled (This improves productivity of Metaframe server)
  2. Hide these specified drives in Windows Explorer – C:, D:, E: (These are local drives to the Metaframe server. This disables viewing local data but still allows clients to run published apps)
- Administrative Templates → Desktop
  1. Hide all Icons on Desktop – Enabled. Prevents access to My Computer, My Network Places, Briefcase, Recycle Bin, etc.
  2. Don't save settings on exit – Enabled. Does not save the client personalized settings
- Administrative Templates → Control Panel. Disable Control Panel – Enabled. This prevents users from accessing all Control Panel Applets
- Administrative Templates → System
  1. Disable the Command Prompts – Enabled. Prevents access to command based utilities or data.
  2. Disable Registry Editing Tools – Enabled. Prevents clients from running regedit or regedt32

GIAC routinely monitors and verifies that GPOs are being correctly applied to the OU that they are assigned. To do this GIAC Customer Support does a

preliminary sign-on with the random accounts of new clients. Attempts to access non-customer information are made and the resulting logs that are generated are pored over to understand patterns to watch for. GIAC is also able to sign on to production servers and with a tool from Microsoft (Resultant Set of Policy) get a read-out of what policies are applying what settings to users who are signed onto the same server. This tool is remote capable which allows GIAC to also use it internally and verify that employees are having their necessary policies applied.

Additional Security

Group Policies address a large percentage of security concerns that GIAC has. However there are certain aspects that require additional considerations. With GIAC being an entirely Windows 2000 based organization, staying current on operating system and other software patches is a big issue. As mentioned earlier GIAC has purchased the third-party software Update Expert to push Service Packs and hotfixes to all servers and workstations. Update Expert is set to check for new OS updates on a scheduled basis of twice per day. The Internal Support group is in charge of monitoring this application to determine when fixes have been released that apply to vulnerabilities found earlier.

GIAC has developed a system by which vulnerabilities that are released or found by Microsoft, Cisco, Computer Associates, BugTraq and other vendors or security postings are monitored and assessed internally. The Internal Support group is in charge of this process and elevates the status of issues to management as needed. Vulnerabilities are rated on a scale of 1 to 4. Level 1 vulnerabilities are considered to be a hoax or of no impact to GIAC. If a vulnerability gets a rating of 2 the fix is scheduled to be applied at next convenience. This could be during a scheduled downtime of a server or router. If it gets a rating of 3 the fix must be applied to the device in question within 48 hours. If a rating of 4 is assessed the fix is to be applied at the absolute soonest possible time, even if that means affecting Service Level Agreements with clients.

Physical access to GIAC's infrastructure is of particular concern due to the fact that all production environments are located in rarely-supervised environments. Because of this all servers and networking equipment for production domains are kept behind locked, steel doors within leased space of the ESUs. Only Customer Support and Data Communications employees have access to keys for these doors. For the internal domain all IT equipment is kept in temperature controlled, raised-floor server rooms. Access to these rooms is given to only four employees and is controlled by magnetic swipe cards. All employees are required to have these cards for any level of access to corporate offices, but only four have the added access to server rooms.

GIAC has also implemented a Host Intrusion Detection System (HIDS) and a Network Intrusion Detection System (NIDS). Even though GIAC maintains robust corporate firewalls, some attack attempts can masquerade as legitimate data communications. To catch these attempts GIAC has chosen a HIDS/NIDS

combination from Cisco Systems. The HIDS software is installed as a client on all GIAC servers and based on the nature of the server is hardened appropriately. These clients report to a centralized Console server located in Lincoln. HIDS enable servers offer another level of protection from known attacks against specific software functions, hacking attempts such as buffer overflows and Trojan horses that can sometimes not be detected by Anti-virus software or firewalls. The NIDS is a hardware based product that scans network traffic, protecting against Denial of Service (DOS) attacks, worms, and other software attacks. It also monitors for probing techniques like port scans and ping sweeps.

Last, but certainly not least GIAC has addressed what may be most companies' biggest security concern: their users. As is the case with any company, GIAC employees are likely to be the first ones to notice in the event of a hacking attempt. This is why GIAC encourages all employees to report any suspicious behavior to the Internal Support or Data Communications groups immediately. Employees are given access to electronic copies of Incident Response Notifications to do just this. As part of the employee hiring process and GIAC's internal Continued Education program, employees are given the warning signs of hacking activity and instructed on what do to in such cases. This process is mandatory for all employees since social engineering techniques could be used on any employee to gain access to company information.

It is important for GIAC IT employees to maintain a good rapport with internal and production customers for both simple business reasons and forward security thinking as well. If a customer or employee feels the least bit apprehensive about reporting an inconsistency experienced on the company network, a chance to avoid or prevent an attack may be missed entirely.

References

Fossen, Jason; Windows 2000/XP Group Policy and DNS; pages 99-102; SANS Institute, 2002

Microsoft Corporation; Microsoft Knowledge Base Article 279890; http://support.microsoft.com/default.aspx?scid=kb;en-us;279890

US Department of Energy; Computer Incident Advisory Capability; Information Bulleting – Creating Logon Banners; http://www.ciac.org/ciac/bulletins/j-043.shtml

US Department of Defense; Password Management Guideline; http://security.isu.edu/pdf/cscst285.pdf

Last Updated: July 27th, 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