GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

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

Secure Windows 2000 Infrastructure Design for Giac Enterprises

Edmundo Farinas
April 28, 2003

GCWN Practical Assignment Version 3.1

Summary

The purpose of this paper is to document the design and implementation of the Giac Enterprises secure Windows 2000 network. This paper explores how the company is logically and physically organized and how it operates, required steps to design and implement an Active Directory infrastructure that meets their functional and security requirements.

A brief description of the company is presented in order to show the nature of its business and to serve as the starting point for the network and Active Directory design, which is then used to implement security through Group Policy.

In some cases, where risks mitigation is not achieved through Group Policy, alternate mechanisms are described and explained to complement the security of the Giac Enterprises corporate network.

Description of Giac Enterprises

Giac Enterprises is a company that creates and publishes state-of-the-art online computer games.

The online games developed by Giac Enterprises incorporate the most recent technology available, which has been internally developed by this organization and is considered one of the best ones in today's market, offering to the players near-real experiences. The technology used by their games has been subject of several awards by recognized organizations in the gaming world due to its uniqueness. Their computer games are always in a process of constant improvement, which is mainly achieved through its efforts and investments in gaming research and development. That is the reason why Giac Enterprises differentiates from the rest of its competitors.

In order to increase market penetration, the company has strategically decided that the platform used at the client part of the games created by Giac Enterprises will be Windows (any desktop version), and a proprietary operating system will be used at the server portion of the software. The server portion of the software is being hosted at a third party network that provides enough and highly available resources.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Giac Enterprises Organizational Structure

The organizational structure that supports the operations of Giac Enterprises is arranged in the departments described below:

Research & Development

It is considered the core of the organization because the technologies and products that have made of this company a successful organization are created and coded in this department. Investigation and development of graphical designs, audio and user interfaces, to name a few, are some of the activities performed in this department.

This department is responsible for:

- Investigating, improving and developing new technologies
- Developing new products (games) and improving the existing ones, based on the new discovered and improved technologies
- Incorporating into Giac Corporation products, new functionalities based on its customers' feedback.

The result of every research and development effort is considered the most important asset of this organization, being cataloged as confidential information.

The information regarding the employees working at this department (name, e-mail, phone number, etc.) is not confidential but it has been classified for internal use only, so it cannot be published at any public site.

Sales and Marketing

This department guarantees the delivery of the company's products to its customers. At the same time, this is the main point of contact with such customers, gathering feedback on existing products to make Giac Enterprises able of satisfying its customers and increasing its market share. This department is in charge of managing the information of the company's customers, which has been classified for internal use only. An ERP system has been acquired to help this department perform its duties.

This department is responsible for:

- Studying the tendencies of the online game market
- Managing all the game distributors
- Being the point of contact and "representing the customers" (players) in the organization, when functionality needs to be improved

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Human Resources and Finance

This department provides support the organization from within, helping the other departments as well as its members. Management of employees' information and their benefits, payroll, internal accounting and suppliers are responsibilities of this department. The before mentioned ERP system has been acquired to help this department perform its duties.

Operations & Support (O&S)

This is the department in charge of the daily support of the corporate network and its components as well as the operation of the infrastructure used for servicing the online gamers (hosted in a third party colocation). Management and maintenance of the operating system, e-mail, network and computer hardware of Giac Enterprises' systems are some of the most important duties carried by the personnel in this department.

The personnel of this department require administrative privileges, as well as special accesses mainly because they provide assistance to all the other departments regarding Giac Enterprises network and its use.

Quality Assurance (QA)

Each of the products created by the Research & Development department, passes through a rigorous quality assurance process in order to guarantee that Giac Enterprises software meets industry standards and at the same time it includes market's requirements, with the less possible amount of software bugs.

Additionally, this department is responsible for:

- Guarantying certain level of compatibility between user's operating systems and the online games developed
- Keeping at minimum the number of software bugs at every release and version of the company's applications
- Reproducing errors and testing the fixes of the reported bugs of every Giac Enterprises' product

The QA group requires certain flexibility at their test environment in order to simulate all the common interactions of the real online gaming world and its users, for every single product to be tested.

In most of the cases, the information managed by this department is exactly the same that every online gamer has access to, so there is not specific privacy issues.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

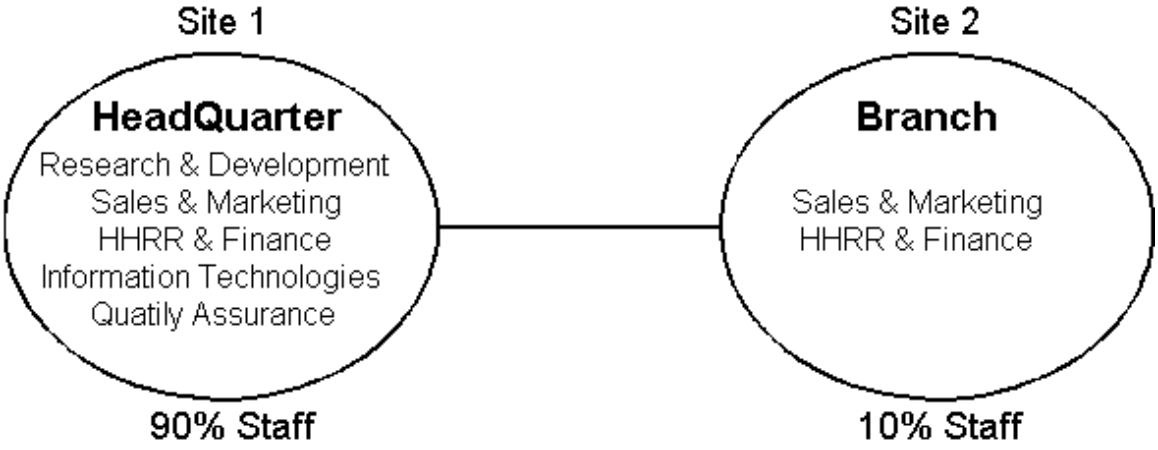
Employee and Physical Distribution

At this moment Giac Enterprises has 82 employees, distributed as follow:

Department	Headcount
Research & Development	45
Sales and Marketing	14
Human Resources and Finance	6
Operations & Support (O&S)	7
Quality Assurance (QA)	10

It has been estimated a Giac Enterprises' headcount growth of no more that 30% in the short-medium term.

The company is located in two (2) geographically distant localities, each one supporting the necessities of its zone. The complete Research & Development department, as well as the O&S and QA departments, are located in the Headquarters. The other departments ("Sales and Marketing" and "Human Resources and Finance") have presence on both localities.



The personnel distribution at present time is at follows:

	Headcount	
Department	**Site 1 (Headquarter)**	**Site 2**
Research & Development	45	0
Sales and Marketing	6	8
Human Resources and Finance	4	2
Information Technologies (IT)	7	0
Quality Assurance (QA)	10	0

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Giac Enterprises Operation

- Each department needs to communicate through electronic e-mail to the rest of organization as well as to Internet. Web access to the Internet is mainly required for Research purposes by the Research & Development department as well as the Sales and Marketing one. The QA department also requires Internet access in order to perform its regular duties.

- In both localities, file sharing is required for small to medium amounts of data in order to allow developers and researchers as well as the other employees of the organization, share the company information they manage and use. Print usage is not a 24 x 7 service but in certain days of the week, high print loads are submitted. The Research & Development team does not require sharing files outside their department. For the R&D team, this level of privacy is a key issue to address in the network implementation.

- Due to budget restrictions, Giac Enterprises would like to be able to remotely manage the Site 2 networks from the Site 1.

- Due to Giac's Enterprise business, temporary personnel (interns and contractors) are commonly present at Site 1.

- Because of the importance and sensitiveness of the information handled by the Research & Development department, the company has decided to locate them in an office inside the Giac Enterprises premises at the Headquarter building but physically isolated from the rest of such location through physical access control mechanisms.

Network Design and Diagram

When designing a Windows network, its physical and logical design is key to lead to a secure implementation. Details like placement and role of each server at the sites' networks as well as the Active Directory (AD) structure will dictate most of the Giac Enterprises' corporate network security features and restrictions.

In order to name the servers for Giac Enterprises network and to illustrate the network diagram, the following server naming standard is defined:

AA-n-m Where,

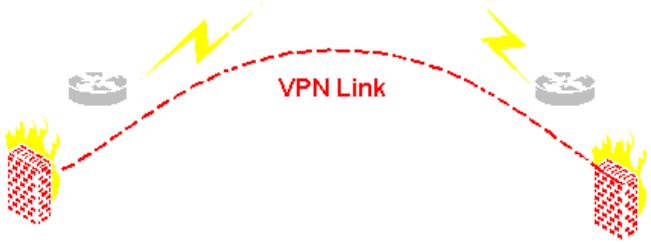
AA represents the server (any two letters A-Z are valid)
n represents the site (1 or 2)
m the server number (1 or greater is case there's server redundancy)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The networks will also follow a naming standard:

NNN-n-m Where,

NNN represents the named network (any three letters A-Z are valid)
n represents the site (1 or 2)
m represents the network number (1 or greater)



Site 1 (Headquarter)

This is the site holding the majority of personnel, so it has been defined as the network core. For redundancy purposes, dual Domain Controller Servers (DC-1-1 and DC-1-2) are provided.

Based on the number of users in this site and their needs, two (2) File and Print servers (FP-1-1 and FP-1-2) will be used at this locality. One of the servers (FP-1-2) will be dedicated to the Research & Development department, because of the importance and sensitiveness of the information their handle.

At this site, a firewall will create multiple logical and physical zones (demilitarized zones), controlling and logging access between them.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Due to the type of access and interaction that will be needed for these servers, three of them (DC-1-1, DC-1-2 and FP-1-1) will be connected on the same logical and physical zone (LAN-1-1).

A demilitarized zone (DMZ-1-1) will hold the mail server (MS-1-1) and the public web server (WS-1-1). By the nature of the services of such servers, this zone will be visible (just the required services) from the other locality (Site 2) and/or any place of Internet. Such visibility will be controlled by the firewall based on a combination of source address(es), service(s) and/or port(s) and destination address(es). Additional security mechanisms such as strong authentication will be provided for user access purposes.

Two separate zones (LAN-1-1 and LAN-1-2) will connect Giac Enterprises employees to the corporate network. One of such zones (LAN-1-2) will be for exclusive use of the Research & Development Department. Such access segregation will provide this department with a mostly-isolated environment, satisfying the requirements of privacy in their work environment. They still will be able to access other network resources as well as communicate with other people via electronic mail just as required in order to let them perform its duties.

The communication network (LAN) at this site will be created through Fast Ethernet Layer 2 switches, providing up to 100 Mbps of bandwidth for every single active component with multiple collision domains.

Access to and from the various networks will be controlled by the previously mentioned firewall in conjunction with anti-spoofing control measures such as port protection and mac address filtering at the switches. Administrative changes to the network configuration, layout and connectivity will require assistance of the O&S team, mitigating the risk of external/internal intruders accessing private information and resources through ip and mac spoofing.

Site 2

This site will hold a few employees. A single Domain Controller (DC-2-1) will be used in this locality. A single File and Print Server (FP-2-1) will be used as well in order to serve the small population of this site.

Both servers (DC-2-1 and FP-2-1) will reside in the internal LAN (LAN-2-1). A second firewall will control access to and from such zone, allowing only the strictly required interactions.

The zone defined as LAN-2-1 will also be used for users at Site 2 in order to connect to the corporate network.

From the business continuity point of view and for contingency purposes, Site 2 (with some restrictions) could serve as the alternate site for Site 1.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Just like with Site 1, the communication network at Site 2 will be achieved through Fast Ethernet Layer 2 switches. The same anti spoofing measures will be taken for this network.

Hardware and Software Configuration for the Servers

Hardware considerations

Each server will be installed with a redundant set of components to minimize the risk of service interruption due to hardware failures. The server platform has been chosen to provide an excellent performance as well, considering medium to high loads.

Regarding hard disk drives and its use, the following table details the suggested assignation and configuration for each type of servers, based on its role in the network.

		SERVERS			
		DCs	FPs	WSs	MSs
Number of hard disk drives	**Disk Protection level**	**Disk assigned for:**			
2	Mirror	OS	OS	OS	OS
2	Mirror	Transaction logs	Print Spooling	Web Server Logging	Mail server logging
3	Raid 5	Active Directory	User files	Web content and applications	Users e-mails

- Size and speed of any current hard disk drive will meet Giac Enterprises storage and response time requirements.

- Every single server will have dual Fast Ethernet interface cards, configured in teaming mode for high availability purposes.

Software Considerations

- Due to the fact that this is a completely new installation and in order to have the latest software features and security fixes, all servers will run a version of Windows 2000 (Windows 2000 Advanced Server) as well as all Workstations (Windows 2000 Professional Server), all with SP3 and the latest security patches and hotfixes. This will make of Giac Enterprises' corporate network, a pure Windows 2000 deployment (no Windows NT compatibility required) so all DCs will run in native mode.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- For budgetary reasons the e-mail server used at Giac Enterprises won't be a Microsoft Exchange Server. Such decision will simplify the design of the Windows network and there won't be integration issues. This server will run a standard POP3 and SMTP enabled mail server software.

- Regarding the web server and because it is a new installation, it will run the latest Microsoft Internet Information Server (IIS 5.0) version, with the latest available patches applied. Budget restrictions did not affect this decision because of the MS IIS licensing schema.

Additional considerations

- Each location will access the Internet through a symmetric link of enough capacity, based on each site requirements (T1 = 1.544 Mbps at each site).

- The Internet will be used to provide user access (inbound and outbound services) as well as Windows traffic replication. In order to protect the replicated traffic (traveling through a non trusted network – the Internet) there will be a logical VPN Link (through the Internet) between Site 1 and Site 2, having two VPN enabled firewalls, one at each locality, as its endpoints. Additional security measures such as traffic filtering at the DCs, proper hardening and physical security of the servers and network elements will allow this replication to be performed through the Internet in a secure way.

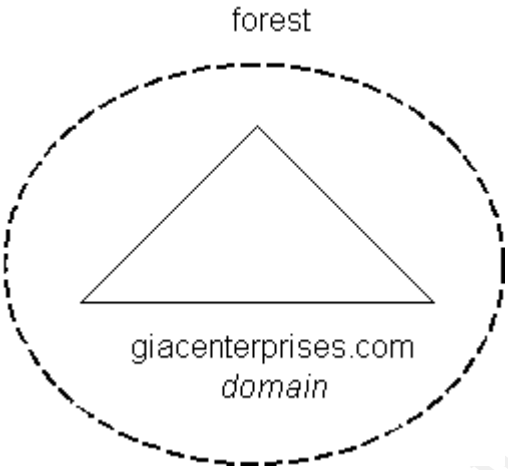
- User services such as email and web will be provided to Site 2 from Site 1. No user services will be provided from Site 2 to Site 1.

- Desktop IP assignation for both sites will be static.

Active Directory Design and Diagram

There will be a domain for Giac Enterprises corporate network. Its name will be giacenterprises.com and all the users and most of the computers will be inside such domain. Based on Giac Enterprises requirement and in order to keep the design and implementation simple, this will be the only domain used at the corporate network.

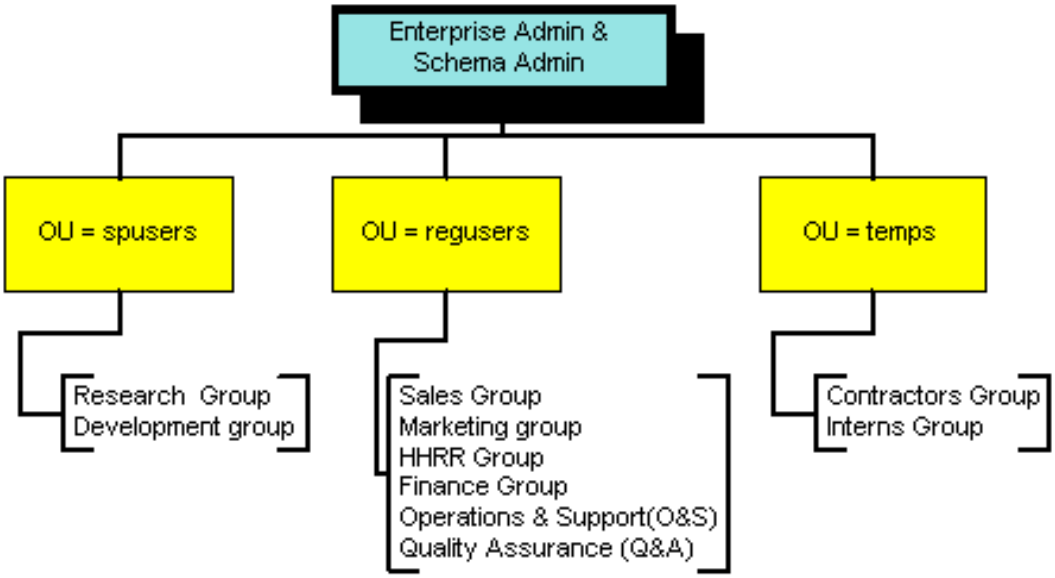
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



In order to protect the domain just defined for the corporate network from the web and mail server, the servers located in the DMZ-1-1 (MS-1-1 and WS-1-1) that require interaction from and untrusted sources, will run as standalone servers.

Due to the fact that there's only one domain at Giac Enterprises corporate network and because this is a 100% Windows 2000 network, no Windows Trust relationships of any form are required.

In the enterprise-wide domain created for Giac Enterprises (giacenterprises.com) there will be three Organization Units (OUs) one for the Research & Development, another for the temporary personnel and the third one for the rest of the organization, as depicted below.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Network administration

The fact that Giac Enterprises will use a single domain for its corporate network will provide high flexibility for future growth. Adding new domains to this network will also be possible with not excessive administrative overhead. Active Directory backup and recovery procedures will be the simplest possible, allowing the organization to perform an AD recovery procedure with less effort that a network with multiples domains.

A centralized management model (based on Site 1) will be implemented for this corporation. All network administration duties will be performed remotely at Site 2, whenever possible. This approach might affect administrators' response time at Site 2 but that is how Giac Enterprises has decided to operate its networks.

Delegation at the giacenterprises.com domain will be performed through the various OUs created (regusers, spusers and temps), whenever it is required.

For security's sake, there will be administrative overhead in order to manage the WS-1-1 and MS-1-1 servers, both in standalone mode but the risk of an intruder of compromising the corporate network Active Directory through these too servers will be highly mitigated.

In order to provide enough flexibility to the QA team, they will have enough local privileges at some of their workstations in order to allow them configure and "tweak" their environment as required for testing purposes. Such workstations won't be part of the Windows domain but will reside in a workgroup. In order to mitigate the risk of human error related to this department's duties, such additional privileges will be provided with the assistance of custom MMC snap-ins.

Due to the fact that a non-Exchange server will be used at Giac Enterprises corporate network, there will be an impact in the management of the network, making it more complicated in some cases (user management for example, because it won't benefit from the Active Directory features) and simpler in other situations (because integration issues will not arise).

Performance

Giac Enterprises will implement the simplest Active Directory model: a single domain, so the network administration is not going to be too complicated (due to domain multiplicity).

There is enough bandwidth between the two locations where Giac Enterprises has presence (1.544 Mbps) so replication should not be an issue from the performance point of view.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

There are no multiple levels (sub-domains) at the giacenterprises.com domain so Shortcut Trust does not apply to the Giac Enterprises Windows network, and there's no penalty associated to such Trust relationship.

The use of multiple Organizational Units and GPOs (applied to such OUs) could be seen as a potential source of performance degradation. In the case of Giac Enterprises Active Directory design, there're not multilevel OUs and only one GPO will be associated to each Organizational Unit so the performance won't be badly impacted.

Security

The domain giacenterprises.com will include information about the most important group in the organization, the Research & Development department. The information about their researches and developments will not be stored at the Active Directory so its security will not directly depend of AD replication.

Information about the Research & Development users (such as name, e-mail, phone number and other) do is stored at AD but at replication time, it will not reach the public servers directly so there is no security issue on using a single domain for these users and the rest of the organization.

This model assumed that physical security in both locations is provided for all the Domain Controller Servers.

From the business continuity point of view, Site 2 has been though as an alternate Site for Site 1, so Site 2 domain controller (DC-2-1) will also be a Global Catalog.

Active Directory replication and Site 2 access to web and e-mail services will occur through the Internet, so appropriate encryption levels as well as traffic filtering will be defined at the VPN enabled devices (firewalls in this design) in order to protect it. To fix the ports used when traffic is replicated, making it simpler to filter please refer to Q224196.

For redundancy purposes, at Site 1, both DCs (DC-1-1 and DC-1-2) will be Global Catalog Servers.

Policies applied over the defined domain as well as the OUs will be detailed in the following sections.

Group Policy and Security

Based on the Group Policy Object (GPO) LSDOU processing order, the Default Domain Policy will set the security baseline for securing the corporate network in the giacenterprises.com domain. Based on Giac Enterprises needs, the security requirements

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

for this policy have been defined as medium to medium-high. The Default Domain Controller Policy will help the organization to apply the specific security measures at the Domain Controllers.

Basic Group Policy

Default Domain Policy

The values at this Group Policy Object (GPO) and the ones at all the other GPOs described in this document will be forced to the desired values in order to provide the required security. This will protect the GPOs to become less secure if an original default secure value is later on set default to a non-secure one.

Additional GPOs will override the Default Domain Policy when higher security settings are required.

Taking into consideration that Windows 2000 has been designed in a way that it makes the Default Domain Policy GPO affects the passwords, kerberos and lockout settings of every single account at the network, any other password, lockout and kerberos policy defined at any other GPO in Giac Enterprises' network, will be ignored by all the domain accounts.

Through this particular GPO, Giac Enterprises will be able to control enterprise-wide use of passwords, forcing the users to change it regularly (every three months) without letting them easily recycle their passwords. Because of the security requirements of the organization, passwords should always be stored with a non-reversible encryption mechanism unless there is any technical constrain forcing to do the contrary (which is not the case for this implementation). Such consideration is also defined and applied through this GPO.

Windows Settings > Security Settings > Account Policies > **Password Policy**		
Feature	**Value**	**Explanation**
Enforce password history	24 passwords remembered (max value)	This setting will prevent users changing their password back to the previous 24 passwords they used before. This number will be enough to
Maximum Password Age	90 days	Three months (at most) should be the life cycle for every user password, limiting its exposure.
Minimum Password Age	2 days	Making it difficult for user to recycle a password by changing it too often (not before 2*24=48 days)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Minimum Password Length	10 characters	At least this amount of characters (10) will be required for every password at the Giac Enterprises to make them not so easily guessable
Passwords must meet complexity requirements	Enabled	To include special and punctuation characters. In conjunction with password length, this setting decreases the exposure to brute force
Store Passwords Using Reversible Encryption for all users in the domain	Disabled	Because CHAP, Radius and IIS Digest Auth are not required at this Windows network.

The lockout settings for this GPO have been defined in order to reduce the likelihood of account security compromises, forcing users to wait for support of the O&S department personnel in case they exceed six bad logon attempts in a period of 30 minutes. If for any reason such support is not provided 12 hours after the account was locked, it will be automatically unlocked without administrative assistance.

Just as the Password Policy, the Account Lockout Policies will be the same for every single domain account in the organization, regardless any redefinition of the settings at any other GPO.

Windows Settings > Security Settings > Account Policies > **Account Lockout Policies**		
Feature	**Value**	**Explanation**
Account lockout threshold	6 invalid logon attempts	6 bad attempts to logon will lock the account, making it more difficult to intruders to guess a password and at the same time mitigating the risk of internal account harvesting
Account lockout duration	12 hours	Medium/High security is required for this policy so waiting for half a day to automatically unlock an account should be enough, having in mind that Denial of Service could arise as a possible side effect
Reset account lockout counter after	30 minutes	If multiple attempts do not reach the lockout threshold, 30 minutes will have to wait the user to start trying to logon again. This measure will deceive potential brute force attackers because of the time required to perform the password

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

		guessing procedure without locking the accounts.

Regarding kerberos settings, through this policy the Default Domain Policy will increase the default values in order to improve the security of the Windows network without affecting too much its performance. These setting, just like the Password Policies and the Account Lockout Policies will apply for every single domain account at Giac Enterprises Windows network.

Windows Settings > Security Settings > Account Policies > **Kerberos Policy**		
Feature	**Value**	**Explanation**
Maximum Lifetime for Service Ticket	300 minutes	Because medium-high security is required. The tickets will be cashed for only 300 minutes
Maximum Lifetime for User Ticket	5 hours	Limiting its exposure but forcing user tickets to be renewed every 5 hours.

Because of Giac Enterprises business, record of potential security events has to be activated for audit purposes. Such records will help the Giac Enterprises trace any intrusion attempts or perform any kind of forensic analysis when a security incident occurs. The audit settings will be set accordingly.

Windows Settings > Security Settings > Account Policies > **Audit Policy**		
Feature	**Value**	**Explanation**
Audit directory service access	Success, Failure	This configuration will enable Active Directory logging
Audit logon events	Success, Failure	In order to record console and remote accesses to Giac Enterprises systems
Audit Object Access	Failure	To enable NTFS, printer and registry changes, where configured
Audit privilege use	Failure	This will help detecting possible potential internal intrusions and misconfigurations

The Guest and Administrator accounts should not be easily identifiable and accessible by intruders, so non-default names should be used to protect both accounts. Additionally, anonymous accesses are commonly an open door to information disclosure so its management should be clearly defined and controlled.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Passwords "resets" are a common source of administrative overhead. In order to reduce such overhead, the users will be notified in advance of password expiration dates, letting them have enough time to change it or request support in order to change it. Company wide security procedures will easily help perform such support in a non-human assisted way.

Lastly, in order to support any legal action to be applied to a pinpointed intruder, a very clear screen message will appear at every system at logon time.

All those setting will be incorporated trough additional Security Options, as follows:

Windows Settings > Security Settings > Local Policies > **Security Options**		
Feature	**Value**	**Explanation**
Rename guest account	<new name of guest account>	Choose a not easy to guess long name. A long password assigned to this user will also help prevent its use.
Rename admin account	<new name of admin account>	To protect the administrative account from disclosure. Obscuring the Administrator account definitely doesn't increase the security but help stopping "script kiddies"
Prompt user to change password before expiration	3 days	This will be the amount of days available for user to change their passwords before expiration.
Additional restrictions for anonymous connections	No access without explicit anonymous permissions	To ensure that only anonymous users will have the right assigned to the Anonymous Users group. Because Giac Enterprises will use a native Windows 2000 networks, this setting will not generate compatibility issues. It will also protect the network from "Null Users Session" attempts
Message Text for Users Attempting to Log On	See "Logon Message" below	This is a good practice not only for Windows systems but also for any company owned system login screen. Such message will also make "hacker apprentices" think twice before playing with a private system.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Logon Message

The following message will be used in the logon window for every server and network device at Giac Enterprises corporate network.

```
Authorized Use Only
|-----------------------------------------------------------------|
| This system is for the use of authorized users only.            |
|                                                                 |
| Individuals using this computer system 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.       |
|-----------------------------------------------------------------|
```

Default Domain Controller Policy

Now that the Default Domain Policy is defined, in order to protect the Domain Controllers at Giac Enterprises' corporate network the Default Domain Controller Policy has to be created.

It is important to note that only the relevant differences between the Default Domain Policy and this one will be explained and detailed in this section.

The Security Options for this GPO will restrict the use of removable media at the DCs, prevent the negotiation of non-secure network protocols (such as LM or NTLM) in order to avoid its use, and keep record of data being backed up and restored at the Domain Controllers.

Windows Settings > Security Settings > Local Policies > **Security Options**		
Feature	**Value**	**Explanation**
Network Security	Send NTLM V2 response only; Refuse LM & NTLM	To prevent potential intruders sniffing the network and capturing data of protocols with weak privacy mechanisms that can reveal users' passwords (with the help of L0pthCrack, for example)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Restrict floppy access to logged-on users only	Enabled	To restrict the use of removable media mitigates the risk of viruses, Trojans, and any other form of malware reaching the DCs, also forcing software updates to be performed through the network
Restrict CD-ROM access to logged-on users only	Enabled	Same as above
Audit use of Backup and Restore privileges	Enabled	Because of human error or bad intentions, due to data restoration important information and program/system files could be overwritten without notice. This setting will keep records of these activities to mitigate such risk.
Change the system time	Disabled	Auditing without a proper time base is sometimes worse than no auditing at all. In order to preserve proper audit timestamping this setting will prevent system time changes.

This GPO will set the logging level higher; making that not only the failure but also the success of especially important events is logged. Such settings will help the organization set a pattern baseline, making it possible to detect abnormal events in the network use and its operation.

Windows Settings > Security Settings > Account Policies > **Audit Policy**		
Feature	**Value**	**Explanation**
Audit account logon events	Success, Failure	This setting will permit the logging of all authentication requests sent by any Giac Enterprises workstations
Audit account management	Success, Failure	To be able to trace account changes, deletions, creations and group assignments
Audit systems events	Success, Failure	This setting will help keeping record of all DCs startups and shutdowns

This Default Domain Controller policy will also go deeper than the Default Domain Policy into the details of logging increasing the security log file size to hold enough information preventing the normal operations if logging fails.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Windows Settings > Security Settings > Event Log > **Settings for Event Log**		
Feature	**Value**	**Explanation**
Shut down the computer if the security audit log is full	Enabled	Here is were functionality at the DCs is sacrificed for the sake of security
Retention Method for security log	Do not overwrite events (clear log manually)	To avoid silly or forced (fake) entries removing the important ones at this log. This will create administrative overhead but might be automated through automated backup scripts.
Maximum security log size	4,194,176 Kb	It is the maximum log size (approximately 4 GB). There will be enough room at the disks to hold this vital data
Restrict Guest Access to security logs	Enabled	Restricting its visibility to untrusted accounts

The IPSEC Policy to be applied through this GPO, sets the negotiation parameters as well as the encryption algorithms to acceptable values in order to provide adequate privacy levels to Giac Enterprises corporate network.

The only traffic that will not be encrypted is the one associated with already encrypted protocols, like HTTPS but only the general configuration is shown below:

Windows Settings > Security Settings > **IP Security Policies on Active Directory**
Based on the Secure Server Policy (filter Action: Require Security), set: • The Diffie-Hellman group to Medium (2) • Re-keying after 30 minutes • 3DES as the only option for Phase I and II (II is the important one). Remove all DES dependencies. • MD5 as the only available data integrity protocol (a little faster than SHA1) • Certificate authentication with certificate revocation checking will be used between peers instead of shared secrets

Additional Group Policy

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

In some cases, the Default Domain and Default Domain controller Policies are too broad to handle specific security requirements for certain groups. That's why additional GPOs are applied to such groups through the help of the additional Organization Units previously defined.

It is important to note that Policy Overrides is not required to be used at any GPO in Giac Enterprise corporate network. Inheritance is not being block as well, so issues in this particular area should not arise.

RD GPO (for the Research & Development OU)

The Research & Development department is were the internals about the company's product is managed in a daily basis, so security is a very important issue to address for them at GPO level.

This OU will inherit the kerberos, passwords and lockout policies from the Default Domain GPO, however, additional options will be used in this GPO in order to tighten its security.

Just as stated before, this department will be physically isolated from the rest of the company and their members will use resources dedicated to the solely purpose to serve them. The RD GPO will restrict the use of certain available network features and will facilitate the enforcement of the strong authentication, required by the personnel working for this department.

Settings like access to removable devices and restrictions to change local time and others will also be included in this GPO, but even though those are not inherited through the Default Domain GPO, such setting are not going to be described in this section because all of them were described before (in the Default Domain Controller section)

The most important differences between this GPO settings and the Default Domain Policy's ones are shown below.

Windows Settings > Security Settings > Local Policies > **Security Options**		
Feature	**Value**	**Explanation**
Smart Card Removal Behavior	Lock Workstation	All employees at the Research & Development department will have to have a Smart Card. This policy will provide them with strong authentication. In case their card is removed, the workstation they removed it from will automatically lock
Deny Access to this	**Groups:**	To avoid those groups to access the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Computer from the Network	**Contractor and Interns**	most sensitive workstations.

Regarding access through Internet Explorer, the idea is not to compromise security by any functionality not required by this department, like changing the browser access settings and automatically storing passwords.

User Configuration > Administrative Templates > Windows Components > **Internet Explorer**		
Feature	**Value**	**Explanation**
Do not AutoComplete to save passwords	Enabled	This option disabled will allow impersonation of someone else at almost any web site
Disable Changing certificate Settings	Enabled	This will not prevent user from importing certificates but would now allow them to modify any already existent
Disable Changing Automatic Configuration	Enabled	To prevent the configured automatic browser updates being modified
Disable Changing Proxy settings	Enabled	To prevent users changing the way they should access the Internet

temps GPO (for temporary employees)

For this case, where temporary personnel will provide their services to Giac Enterprises, a new GPO will extend the Default Domain Policy in order increase company's security due to these untrusted users.

Such temporary employees will not have rights to perform configuration changes at the workstations they will use. They won't be able to access their computer through the network, access removable devices and change Internet Explorer access configuration, just like the R&D employees.

They wont have access to neither the control panel nor the run option from the start menu. They won't even have rights to browse the Windows network or forcibly terminate any process. All those previously mentioned setting will make almost impossible for them to change any setting, mitigating the risk of connecting temporary personnel to the corporate network but it will definitely create administrative overhead for the O&S department in the support duties of these workstations and its users.

The most distinguished settings of this GPO as shown below.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

User Configuration > Administrative Templates > **Start Menu & Taskbar**		
Feature	**Value**	**Explanation**
Remove Run Menu from the Start Menu	Enabled	Making it complicated for any temporary user running command lines, the passing of additional parameters to change the behavior of a particular application (this is a GUI only limitation)
User Configuration > Administrative Templates > System > **Logon / Logoff**		
Feature	**Value**	**Explanation**
Disable Task Manager	Enabled	Prevent processes and applications to be abruptly terminated by the temporary personnel
User Configuration > Administrative Templates > **Control Panel**		
Feature	**Value**	**Explanation**
Disable Control Panel	Enabled	This will prevent one of the worst nightmares of Windows administrators
User Configuration > Administrative Templates > **Windows Components**		
Feature	**Value**	**Explanation**
Remove "Map Network drive" and "Disconnect Network Drive"	Enabled	Limit temporary users mapping other sources or substituting the authoritative sources for the network drives
No "Computers Near Me" in my Network Places	Enabled	Limiting what the temporary personnel can see from the network
No "Entire Network" in my Network Places	Enabled	Limiting their scope from the entire corporate network

Additional Security

There are certain security features of a corporate network that Giac Enterprises should incorporate in order to have a robust Windows network. Some of those features are present in Windows but are not applicable through Group Policy; some others are just best practices for any networked organization, connected to the Internet.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Server Hardening and Minimization

By default the way most of the software is installed is good for functionality purposes but not for security. The mail and web servers (MS-1-1 and WS-1-1) will be exposed to a wild environment, the Internet. The other servers (DCs and FPs) will be connected and accessible through the corporate network. The firewall is a good friend but it cannot be the only line of defense. Just think what could happen due to failure or misconfiguration.

Proper software minimization as well as OS and application hardening have to be performed before connecting any system at their networks. Very good Microsoft Windows 2000 hardening guides can be obtained from the NSA at http://www.nsa.gov/snac/win2k/index.html .

Antivirus software

Almost every day a new virus is released and the Microsoft platform is the target and/or where the majority of infections occur. Use antivirus software at least at every workstation and mail server (the virus preferred entrance door), update its signatures at least once a day and perform routine scans. The corporate version of some well known antivirus also provide features to help administrators initiate remote scanning, receive alerts of viruses found and check signature update status at every computer in the network. Just keep an eye on how these new functionalities could unadvertedly affect the security of the corporate network.

Tape Backup

This is one of the most important security measures of every system. To make backups is important but it is more important to test and know that the backed up files and directories can be restored. Use a good backup software and test your recovery procedures regularly.

Instant Messaging Tools

When it comes to instant communications, users are reluctant to change. Once they're used to an specific IM client, a state-of-the art Secure Enterprise IM the company may acquire in order to protect users' communications is almost useless. These family of collaborative tools are a very important part of every day. Giac Enterprises should set IM policies from the beginning to avoid user resistance to change.

Internet Web Browsing / Active Content Filtering / Web Cashing

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

When a user is browsing the Internet, desktop computers are exposed to malicious web sites or with inappropriate content to which sometimes the users can get, even without noticing it. Sometimes it is an extra character at the URL and some others are common typing errors that are registered as valid web addresses. Sometimes users just want to get to those sites. The only way to avoid users accessing inappropriate sites is using an Active Web Content Filtering solution. Certain solutions can be incorporated in the organization in conjunction with a Proxy Servers (like the Microsoft ISA Server), where web cashing is also a desirable available feature to speed up page loads and save bandwidth.

Use of an file encryption mechanism

The Research & Development users should encrypt all their sensitive information, through the Windows Encrypted File System feature or via any other well-known method such as crypto tokens/cards or specialized software for end users file encryption.

Intrusion Detection Systems (IDS)

It is amazing how many people have the time and access to technology resources to perform manual or automated procedures to find and exploit vulnerabilities of Internet and non-Internet accessible systems. An Intrusion Detection System will open your eyes to let you see how your systems and networks are constantly scanned and probed, not only from outside the organization but also from within.

At least the Internet exposed servers (mail and web in this paper) should be "protected" with the help of an IDS. An excellent open source Network Intrusion Detection System (NIDS) called Snort can be found at http://www.snort.org/ .

Learn from other's experience

There's not a recipe for security common sense not even a way for most of the companies how to perform trial and error at every single configuration option of the products a company might have. Refer to trusted and well-known sources of security advice, such as the SANS/FBI Top 20 List (http://www.sans.org/top20/#index) in order to understand and know how to prevent the most successful Windows attacks.

References

The definitive guide to Windows 2000 Group Policy
http://www.fullarmor.com/ebook/read/

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Step-by-Step Guide to Configuring Enterprise Security Policies
http://www.microsoft.com/windows2000/techinfo/planning/security/entsecsteps.asp

Best Practice Active Directory Design for Managing Windows Networks
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/ad/windows2000/plan/bpaddsgn.asp

Alistair G. Lowe-Norris, 1st Edition January 2000 **Windows 2000 Active Directory**
http://www.oreilly.com/catalog/win2000ads/chapter/ch08.html

How to Restrict FRS Replication Traffic to a Specific Static Port
http://support.microsoft.com/default.aspx?scid=kb;en-us;319553

MCSE Self-Paced Training Kit: Microsoft Windows 2000 Active Directory Services
Second Edition, August 2002, Microsoft Press

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.