Global Information Assurance Certification Paper

GIAC Securing Windows Certification (GCWN)

GCWN Practical Assignment (v3.1)

Option 1 – Design a Secure Windows 2000 infrastructure

"Secure Windows 2000 design for the GIAC Organisation"

By: Gordon Crease

September 2002

Foreword

The majority of the contents of the following document have been sourced from a great variety of reference points. It is not the intention of the author to present the information or design ideas as wholly original even though specific references are not noted. A list of the articles or books referenced as part of the document development is presented at the conclusion of the assignment. The fictional organisational design is pieced together from these sources.

All work was completed on a Laptop computer, which has slightly affected some screenshots, and limited some detailed implementations.

Introduction

Option 1 of the Practical Assignment version 3.1, *Design a Secure Windows 2000 infrastructure,* has been attempted. The assignment includes the design of a fictitious organisation known as GIAC. A network design is shown that provides the basis for the companies activities.

The organisations information management is worked around the Windows 2000 operating system and uses the Active Directory option as the key to applying the organisational security principles via Group Policy. Thus, the document describes the overall system configuration in relation to users, computers and network interconnectivity. A brief explanation of each of the components is given.

There is a section on the design of the Active Directory itself, indicating the organisational structure and how it is represented in the directory schema. A section detailing two of the primary Group Policy configurations has also been completed, and this is followed by the examples of two other Group Policies that are configured in the fictitious organisation.

A final section completes the documentation, and is aimed at providing additional guidelines for securing a network. These are non-Windows specific processes that could, and in many cases should, be applied to the administration of any network.

THE GIAC ORGANISATION **4**

THE BUSINESS 4
THE PRODUCT 4
STAFFING/ROLES 5
BUSINESS UNITS 6
THE NETWORK 6
Overview *6*
Routers *9*
Firewall *9*
Service Network *11*
Internal Network *12*

ACTIVE DIRECTORY DESIGN **13**

INTRODUCTION 13
THE GIAC ACTIVE DIRECTORY 13
DNS 18
REPLICATION 19
FSMO ROLES 21
INSTALLATION OF ACTIVE DIRECTORY. 21
ADDITIONAL SECURITY CONCERNS 23

GROUP POLICY AND SECURITY **24**

INTRODUCTION 24
PRECEDENCE 25
GROUP POLICY MANAGEMENT 26
PLANNING 27
DOMAIN POLICY 27
DOMAIN PASSWORD MANAGEMENT 29
DOMAIN CONTROLLER GROUP POLICY 32
Controlling Services on Domain Controllers *33*
Logging of Actions on the Domain Controller *35*
ADDITIONAL GROUP POLICY 37
Workstation policy *37*
Database and server policy *40*
ADDITIONAL SECURITY 43
Physical Security *43*
Router and Firewall configurations *44*
Host hardening & patching *45*
Auditing *45*

REFERENCES **46**

MICROSOFT WHITEPAPER, *INTRODUCTION TO WINDOWS 2000 GROUP POLICY*, MAY 1999, ... 46

The GIAC Organisation

The Business

The GIAC organisation's information and communication network has been designed to accommodate a growing business that relies on internal research and development to produce a product that can be marketed online. This dependence upon an internally generated product has resulted in an architecture that is split between two separate, hosted sites.

Day-to-day operations of the organisation are completed in a city central environment while a remote site approximately 50 Kilometres from the city centre has also been established where the research and development environment is accommodated. The architectural model followed for the design of the GIAC network is an example of an *Extended Domain Model* due to the fact that there are two sites connected by a Wide Area Network link. This link extends across network nodes that are out of the control of the organization. This choice was made even though the organisation is still relatively small. Still, the IT staff are required to manage and support two physically separated networks.

The Product

The GIAC business is aimed at providing a product to external customers that can be sourced from the GIAC network via a standard browser interface (HTTP or FTP uploads from designated servers), or via a CD, which can be ordered online. A full-time Research and Development team are continually upgrading and improving the product and develop the customer offering in-house. This process is ongoing.

Once the GIAC testing process has been finalised and the product is considered fit for distribution, it is uploaded to the Web server and/or FTP server where it can be accessed and downloaded by customers who can supply the suitable credentials. These are obtained after an order has been received, and payment verified. A timed credential is then sent to the customer via email.

If the customer has a preference for a hard-copy of the product, a CD can also be ordered online. Thus, the GIAC enterprise has a financial aspect that requires that there is the ability to do transactions online.

The product needs to be protected from theft and/or corruption during its lifecycle on the presentation platform. This requires strict controls to be set on access to the Web and FTP servers.

Staffing/Roles

The company is a small but growing enterprise. Presently the GIAC staff numbers are few, however, it is anticipated that in the future some of the roles presently shared by several staff members may be sectioned off to dedicated people. Therefore, it was decided that the initial design of the system would include a role based access model, and staff would be enrolled in (or removed from) the necessary access lists as necessary.

Since GIAC is a fully self-supporting organisation, there is a complete Human Resource Management (HR) and Marketing team, as well as an IT department dedicated to the ongoing upgrading and maintenance of the network and its associated applications. For business reasons, the city office incorporates HR and Marketing while the Research and Development team are located at the remote centre. City centre staff must look after all customer requirements. They deal with all financial transactions, after sales service, as well as any internal organisational needs. They package and prepare the product for access by customers.

The GIAC staff numbers only 40 personnel presently, who share all the roles within the organisation. 30 are permanently at the city office with 8 working in the Research and Development area, and the 2 IT Administrators who are mobile between the two sites, but are mostly based in the city. The Windows 2000 implementation allows for a great deal of remote management of the R&D network.

The GIAC product is developed in an environment that is isolated from the main network. The needs of users in the R&D environment are slightly different from those in the city centre. Apart from requiring a variety of development tools the developers require access to the Internet as an additional research tool. They also need to be able to transfer any completed products to the main office where they are prepared for presentation to eager customers.

Users in the HR and Marketing department will also need access to the Internet, but external customers will also need access into some part of the GIAC network (the Service Network) to download the product. A separate Web server is used to provide static content containing product and organisational information to any wishing to know more about GIAC and it's customer offerings.

Business Units

The majority of organisations have specific units that have been developed to perform specific functions. GIAC is no different, and has the following business units;

- **Human Resource**: Deals with all internal staff requirements
- **Finance & Administration**: Responsible for organisational accounting
- **Customer Service**: Responds to after sales customer needs and product distribution
- **Marketing & Sales**: Development of packaging, promotion and customer contact
- **Technology & Information**: Administration of the information flows and structure of the network
- **Research & Development**: Development, manufacture & product improvement

There are specific hierarchical roles within each of these business units, and these relate to the management structure. Roles associated with members of the different Business Units may vary in some areas, but there are also generic functions that are common across the organisation.

The Network

Overview

The GIAC infrastructure consists of the two physically separate networks (See Figures 1 and 2). Each network is similar in its design in so far as the major components that make up the network have been positioned in a manner that will provide ***defense in depth*** (Symantec, 2002). That is, security does not simply rely on an Internet facing firewall as the only form of defense against misuse of organizational resources. There is also internal filtering of communications between different subnets, as well as access controls applied at individual system resources via Group Policy. Thus, the security policy of the organisation is layered down to the local settings on individual systems.

The network forms a three-tier architecture, with the Service Network forming the first tier (Internet facing components). The second tier provides for the business logic (application servers, domain name servers, mail exchange servers, Domain Controllers and DHCP server), and the databases and associated servers form the final tier. The third tier holds company sensitive data as well as customer information and transactional details. Inter-tier communication is filtered by means of firewall rules or packet filtering (Access

Control Lists placed on the router(s)). All network segments are on Switched Ethernet. A Border router and Firewall located at the city centre are the first lines of defence, as well as the access point into the networks.

For cost and administrative purposes, many of the resources based in the city centre network will be shared and therefore accessible from the R&D network. The shared components will include the Mail relay and Exchange servers, the External DNS located in the Service Network. The R&D network will have its own internal DNS for name resolution, but will share the External DNS for any Internet access requirements, and for access into the city centre Service Network.

Figure 1 *– The City Centre Network*

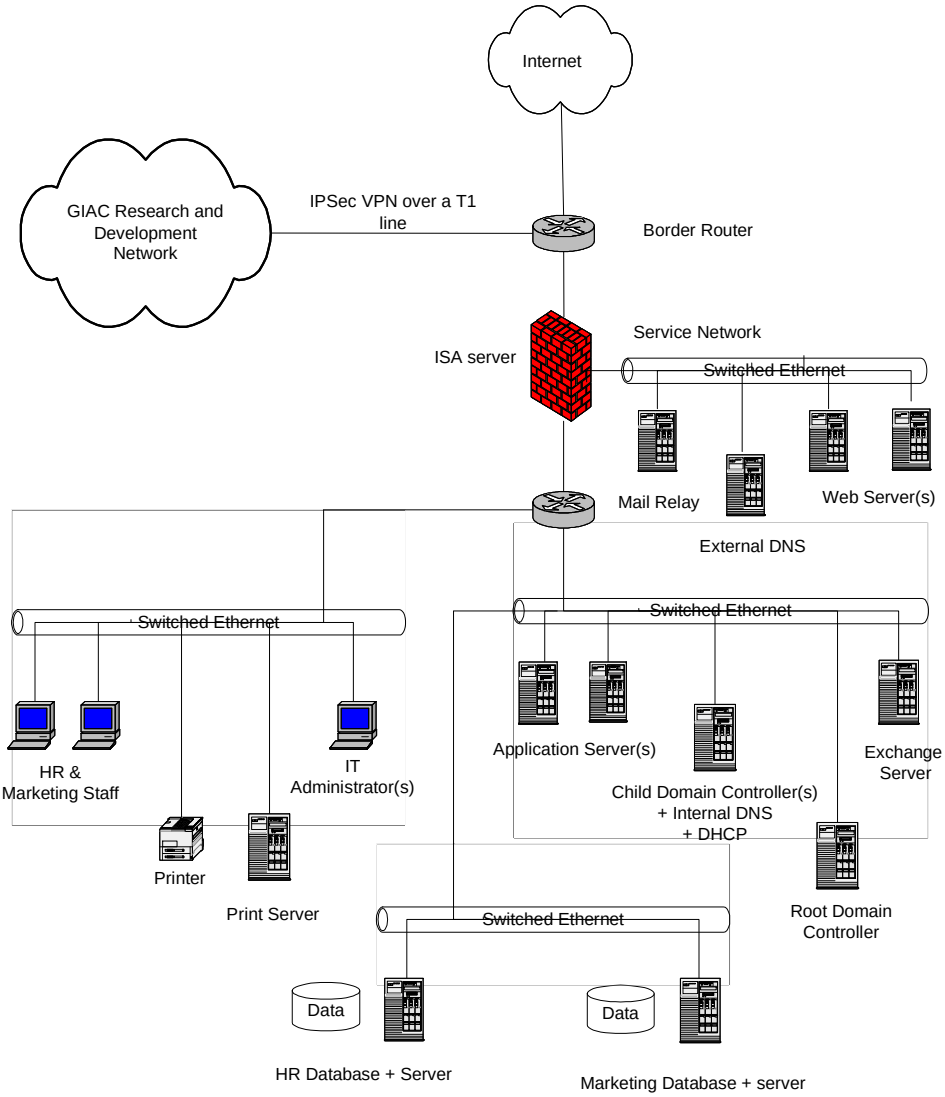
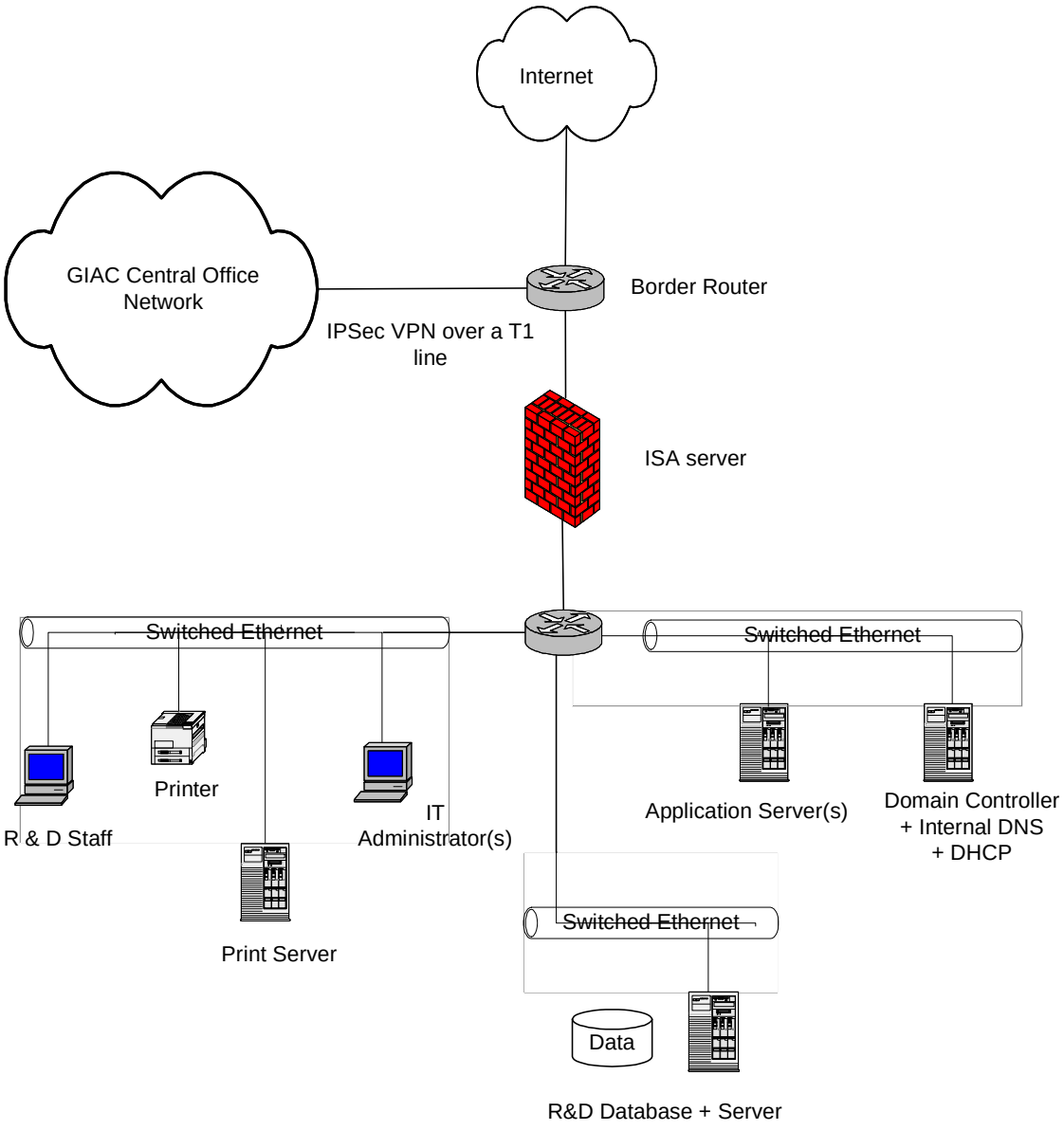


Figure 2 *– The Remote R&D Network*



Routers

Both the border router and internal router are 3660 series routers running IOS version12.2. They were chosen for their versatility and for the ability to support access control lists. Simplicity of management was the prime reason for using identical units for both internal and external routing requirements.

The border routers for each separate physical network have been configured to permit IPSec traffic on the T1 interface - protocol 50 (IPSec Encryption Security Payload) and UDP 500 (Internet Key Exchange). The IPSec VPN will be terminated on the two firewalls that protect the city center and remote sites. All communications traffic flowing between the two sites connected by the IPSec VPN will be encrypted for privacy purposes. All inter-site communications internal to the organization will pass via the VPN.

The border routers have also been configured to reduce IP spoofing by denying communications that originate from any private IP address spaces on the internal facing interfaces (RFC 1918 – 10/8 prefix, 17.16/12 prefix and 192.168/16 prefix). Small services have also been denied. The rule-set remains simple and is configured to filter some of the most obvious unwanted traffic that would otherwise have to be handled by the organizations primary firewall. The rules are mirrored on the firewall, but are only there as a secondary line of protection and should not impact on firewall processing power. Mirroring the router rule-set is not essential, however if the router rules should be compromised for any reason, then the firewall will be able to filter spoofed traffic.

The internal router allows for some segmentation of the internal network and acts as a second *firewall* that partially shields the primary firewall internal interface from internal attacks. In many organisations, these types of attacks are the largest threat to the internal network. The rules placed on the internal router reflect the firewall rules and check for IP spoofing from internal sources. Communication controls can be tightly controlled through the use of port and IP address filtering. Traffic between subnets is also filtered at this point to ensure that internal users access only the hosts specific to their work roles, and in a manner associated with the orgaisationally accepted applications.

All unnecessary services on both the routers are disabled, and the latest operating system patches are applied when necessary.

Firewall

Since the overall design of the GIAC networks has been based on the Windows 2000 product suite, the Firewall chosen is the Internet Security and Acceleration Server (ISA). This is also a Microsoft product which can run on the Windows 2000 Server Operating System with service pack 1 or later – service pack 2 will be used since it will allow for the High Encryption Pack to be installed. High encryption options will be used when configuring the IPSec VPN.

The use of a single operating system across the organisation will hopefully reduce the management complexity that can occur when several platforms conjoin to make up a network. This is an important factor when the limited number of administration staff is considered. However, there is also a down side to the use of a single operating system, and that lies in the concentration of attacks that can occur if exploits are found in that particular system. Regular and frequent monitoring of the security alert groups such as *securityfocus.com* and *sans.org* will help in this area if actions are taken to patch the systems as soon as the solution to an alert is available. Regular monitoring of the Microsoft site is also deemed prudent.

The communication and security of the two networks relies heavily on the two ISA servers. A permanent IPSec Virtual Private Network has been configured over a T1 line which links the city centre network to the remote R&D network. The IPSec VPN will be used as a secure tunnel for Domain Controller replication as well as all other business information that flows between the two GIAC sites. The encryption provided by the IPSec tunnel acts to protect the communications and provides acceptable levels of security and privacy. It will help protect the GIAC customer offering while in transit between the R&D and city centre networks.

There are various ways to configure an IPSec VPN. For GIAC purposes, the tunnel is designed to remain open indefinitely to allow automated DC replication every 20 minutes. Group Policy changes, which are administered from the central office may also have to be pushed to the relevant resources in the remote site whenever they are deemed necessary by the system administrators. Therefore, the VPN authentication is by Shared Key. This is not normally recommended due to the fact that the key is stored in the clear on the device. However, the administrators feel that this is an acceptable risk since there is only a single key and this is stored on the organizations firewall. Also, once the VPN has been established, the authentication key is of less importance since it is not the key used for encryption of any data. Triple DES encryption is used with Encapsulation Security Payload (ESP), SHA1 hashing, and tunnel mode selected.

The firewall also performs the Network Address Translation (NAT) function that allows the System Administrators to use private IP addressing on the internal networks. The choice of a private address space that is not visible to external networks effectively disguises internal systems from the Internet. The Service Network addresses are valid IP addresses and are published to the Internet via the External DNS. A small pool of valid IP addresses are also used by the firewall for internal users to access external networks.

The two sites each have a single class C address range chosen from within the 192.168.xxx.xxx range of private addressing (not shown completely for security reasons). The separation into subnets allows for separate DHCP servers at each site and helps system administrators set up routing and filter rules between the two sites. There is a risk associated with DHCP servers that lies in the fact that anyone with access to the network can plug in a host

with a DHCP client and thus gain access. Independent DHCP servers at each site adds some separation of the R&D and city center networks if such a breach of security should occur. Physical access controls and continued vigilance are always important factors in protecting any network

The firewall rules have been set up to provide a strong protective boundary around the GIAC network. The rules include the implicit blocking of TCP and UDP port access to those specific to a Windows implementation (implicit refers to the fact that only permit rules are actually configured on the firewall). These services that are not permited include the following; NetBios, RPC and Terminal Server. NetBios is not required as part of the single domain Windows 2000 implementation and lack of legacy systems. RCP and Terminal services are not used by the administrators. Other firewall rules are mentioned later. (Fossen, 2002).

Service Network

Each of the Service Network hosts has a valid IP address so that it can be accessed from the Internet. The hosts placed in this network subnet are the working Web server(s) running IIS 5 and Active Server Pages (ASP). They interact with internal network applications to serve up the GIAC product to authenticated customers. They also act as the Business face to the Internet community in general and provide static information about the organization.

There is also a Mail Relay (SMTP forwarder) as part of the Microsoft exchange e-mail system. This relay passes incoming mail to the mail server located in the second tier, as well as forwarding internal emails to the Internet intended systems. Having a simple relay in the Service Network reduces the chances of attacks on the internal email server. Initial content checking and virus scanning can be achieved at this point. The relay is shared by both the city centre and R&D networks, and mail is also forwarded to the R&D network via the VPN. The use of a single relay is both cost affective and administratively less complex, and allows for a single point of content filtering.

An external Domain Name Server is also present in the Service Network. The external DNS is for Service Network host address resolution, and is accessible from the Internet, and by each internal DNS for external resolution of addresses for internal users. The Internal DNS in the R&D network and the city center network are integrated into the Active Directory on the Domain Controllers. The external DNS is not integrated with the AD and also has Dynamic updates disabled. It is a standalone DNS and thus, there is no replication of the Active Directory to the Service Network.

Unauthorised zone transfers can be a problem for many incorrectly configured systems. Zone transfers can be either disabled, or controlled to specific servers. The External DNS in the GIAC is limited to queries to the Internet Server Provider DNS and only publishes the addresses of hosts in the Service

Network, which are needed for e-mail and Web services. There are no zone transfers. The address space is small, and manually administered.

Internal Network

The internal network is connected to a second interface of the firewall via the internal router. The hosts have private addressing in the 192.168.xxx.xxx range, as do the hosts in each of the other segments. Internal communications are filtered at the router as well as at the firewall in such a way that no unnecessary use of company systems is permitted.

GIAC staff have separate work requirements but there are also some basic commonalities. Users have POP3 clients so that they can access the internal Exchange server to retrieve e-mails. This server is configured to send and receive mail from the Mail Relay in the Service Network, but does not have direct access to the Internet, nor can it be contacted directly by users external to the GIAC organization. It is effectively hidden from the Internet by the addition of the mail relay.

The internal DNS (configured on the Domain Controller host) is available for internal name resolution. Only internal resource addresses are available from this host. Users access the Internet via name resolution using the external DNS. Address resolution for external systems is achieved by the internal DNS doing a request to the external DNS in the Service Network, which in turn may do a request to the upstream DNS.

There are some basic organisational requirements. At the city centre, there are the business applications that are needed by the HR, Marketing and Finance departments. These interact with the database servers where all critical enterprise information is stored and protected. Access to these databases is restricted to users via a role based access mechanism. An internal Web server is also used for publishing GIAC staff specific information and business information that is not required to be made available to external users.

There are four Domain Controllers within the city centre network. Two redundant pairs (one for each domain) that form part of the organisation's Business Continuity Plan. Gradually, as the organisation grows and resources can be directed towards infrastructure improvements, more redundant systems will be added as a buffer to element failures. A disaster recovery plan for the organisation is still being formulated.

A fifth Domain Controller is located at the remote R&D site. Replication takes place over the IPSec VPN link between the two networks. The overall GIAC network design allows for users to access system information within the separate networks by authenticating to the local DC or a remote DC if necessary. Thus system bandwidth is reduced under normal circumstances, and the sites can operate relatively autonomously with only a limited reduction in organizational functionality if the link should collapse for any length of time.

Active Directory Design

Introduction

The Active Directory set of services that come with Windows 2000 Server can be used as the directory services for the domain controllers within a network. It forms the basis for all security management features, and is hierarchical in its layout, and uses the Lightweight Directory Access Control Protocol (LDAP) for communications purposes. Along with many other features, it replaces the (SAM) database that is used in a Windows NT4 network implementation, and therefore is the source of user security related information. It stores such in formation as User Account Properties and Passwords, Encryption Keys and Digital Certificates, Groups and Organisational Units and Network Sites and IP subnets (Schmidt, 2000).

Active Directory implementation is not a simple process and anyone considering its use can anticipate the allocation of a large amount of research time to achieve their goals. However, once installed correctly, it will allow system administrators to implement much of the organisation's security policy from a central point. This facility alone makes Windows 2000 Active Directory implementation worthwhile.

Active Directory supports DNS, LDAP and Kerboros and any administrator required to install an AD will also need a basic understanding of the X.500 protocol. Planning before implementation is the key to a suitable design.

The GIAC Active Directory

The implementation of Active directory into the GIAC network allows for the following;

- The use of an Open Standards based management and security tool that is X.500 compatible and enables the application of security rules on individual objects within the database.
- A scalable architecture since the directory can deal with many millions of objects. Well within the requirements of the GIAC organisation.
- A backwards compatible system that can be used with NT4 systems (if required, but not necessary for the GIAC organisation).
- A more available system to all users, no matter where they may be physically located (Schmidt, 2000).

Before installing the Active Directory by promoting the Domain Controllers, it is worthwhile taking a few moments to plan the naming convention for the network and make decisions on how many domains will be suitable for present use, and for possible future expansion.

Many system administrators can add to the complexity and difficulty of their positions by attempting to use every feature available in a new operating system or application. However, simplicity in a design often supports security as it can allow for ease of administration, which in turn allows for simple rulesets and access requirements. Simplicity in Security often leads to improved functionality. Keeping the design as simple as possible is the key to providing a robust and manageable solution.

For the GIAC enterprise, it was decided that a single root domain and one child domain was all that was necessary and would make management a much simpler task and more easily accomplished by the two administrators of the system. If the organisation was much larger with many isolated networks, and had a requirement for single administration of separate areas, it would have been sensible to add additional child domains. In the case of GIAC, only one root domain requires administering, even though there are two physically separate networks. Users throughout GIAC will share the relatively small number of resources available.

The domain name ***generous.com*** was selected as the root domain when the Domain controllers were installed. This design does require additional Domain Controllers that act as a 'place-holder' for the root domain. Although this adds additional hosts to the network it was considered an acceptable cost given the flexibility it provides for expansion.

A single child domain, ***dm1.generous.com*** was created that would encompass the R&D and city centre networks. Further child domains can be created under the root domain in the future if necessary. Thus flexibility is available even with the simple initial design.

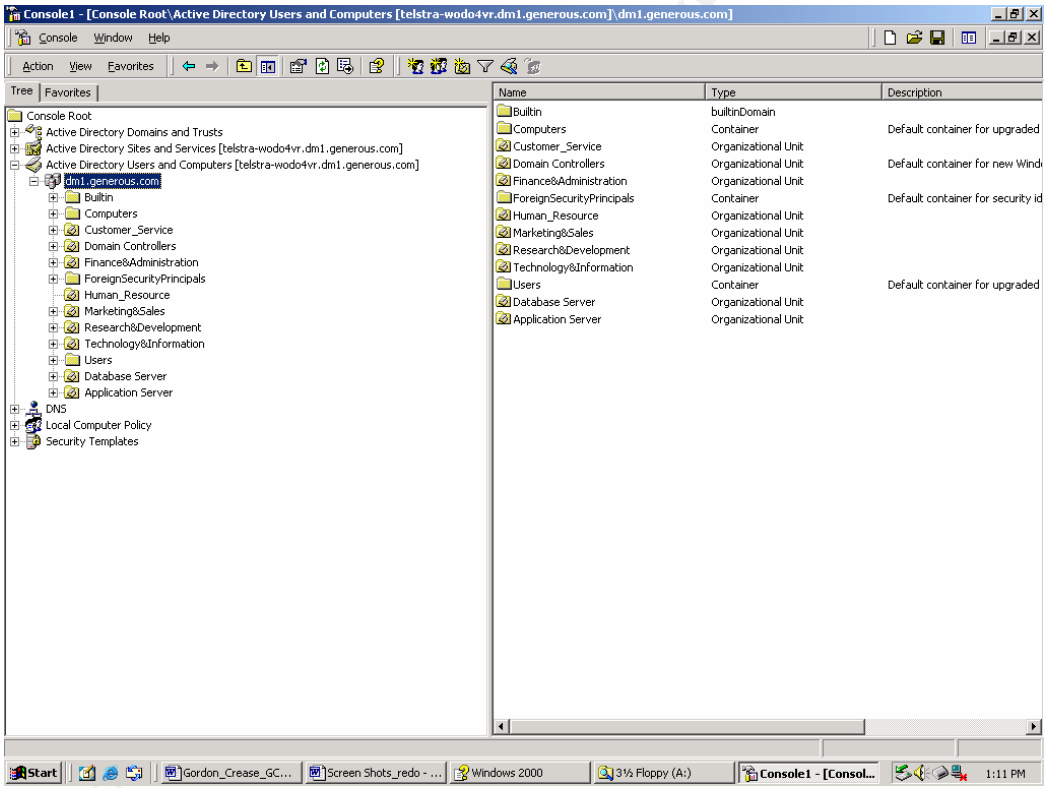
In Windows 2000 terminology there is thus a single Forest with a single tree within that forest. By accepting the concept of one root domain, the designers have also satisfied themselves that a single security policy is adequate for the organisation. The naming system for each of the hosts within the networks is based on the chosen domain name. If the organisation were to grow particularly large, a second root domain may be required. This would form another tree in the forest. Each tree would be separate and could have different security policies applied. See figure below for the GIAC network design.

The hierarchy within the Active Directory has been kept as simple as possible for ease of administration and to make access security implementations also less complex. If the hierarchy passes a nesting level of greater than three, it is worth reviewing the design and possibly restructuring. Nesting up to five levels is still acceptable, but should be avoided (Fossen, 2000). Simplicity will allow administrators to more easily apply the rules that make up the enterprise

security policy. If the hierarchy becomes too deep in its nesting, conflicts can occur and accidental access rights be given to users, or computers when applying Group Policy (conflict issues are also noted in later sections).

It is also an important aspect of the planning process to decide on the Organisational Units (OUs) that will exist within the Active Directory Schema. There is no need to exactly follow the business unit model for an Organisation when choosing the OUs that will be configured. However, it is a simple task to add an OU for each business unit, and then decide if additional OUs might also be of use.

Figure 3 - *The GIAC Organisational Units*



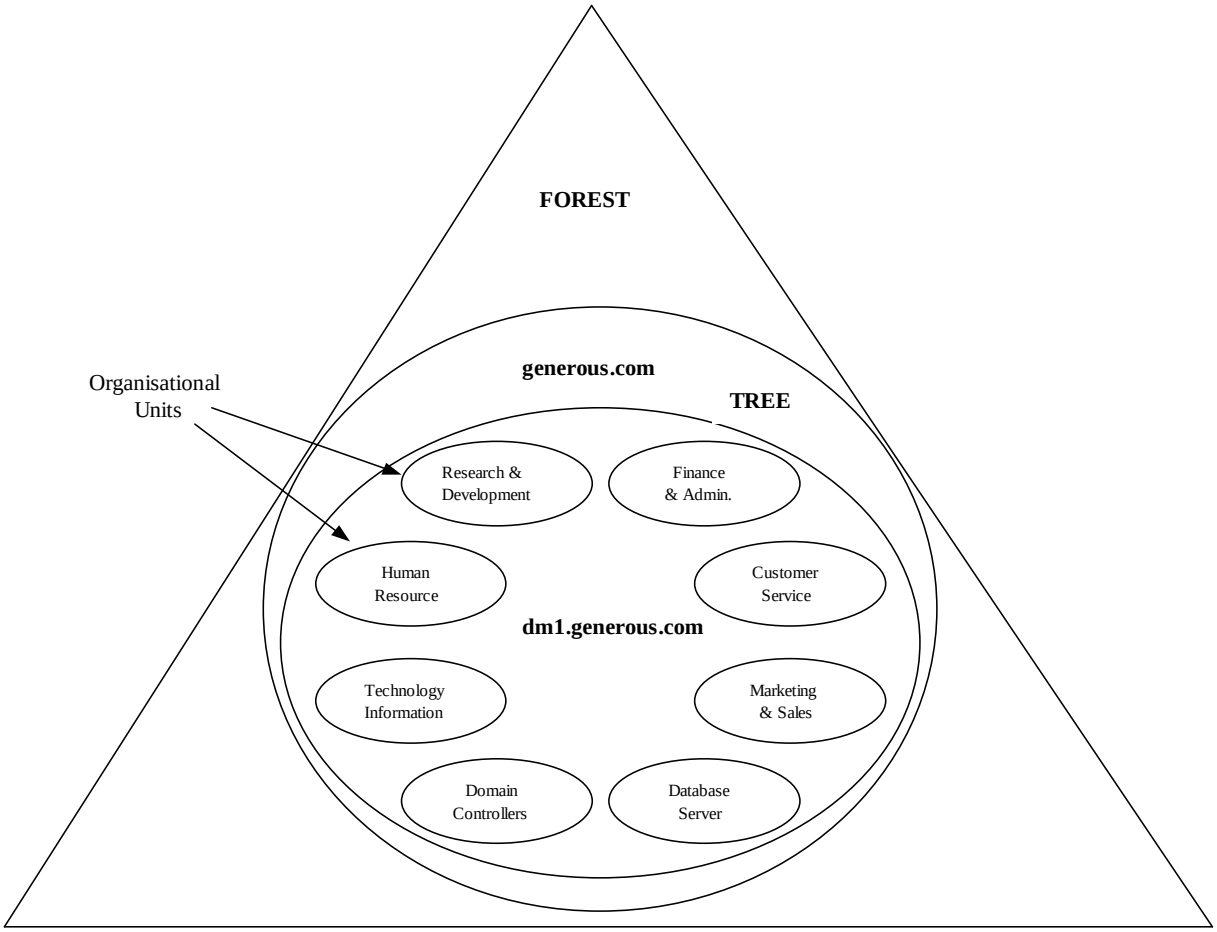
For the GIAC implementation of Active Directory, each of the six Oraganisational Units will mirror the business units described earlier, with the addition of;

- **Domain Contoller OU;** - it is worthwhile ensuring that the key systems in the network exist within their own OU and can thus have policy applied that specifically parallels the role they play in the organisation. There is a default Organisational Unit for DCs that exist as part of the Windows 2000 server basic install. There is also the option of applying one of the available security templates (with organisational specific changes) for adding greater levels of security for these very security sensitive hosts.

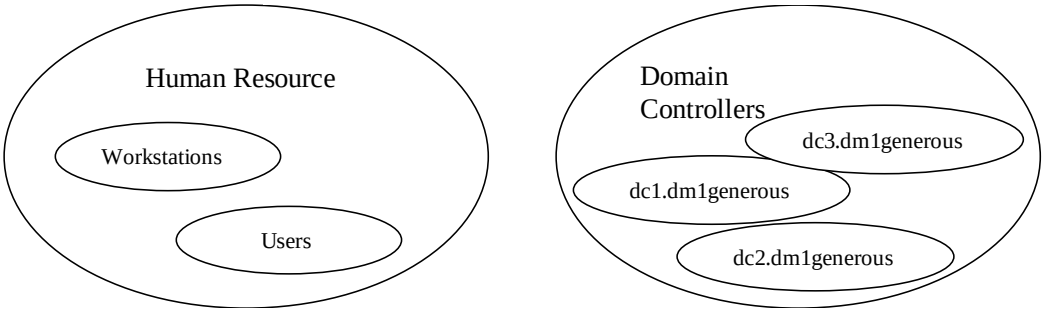
- **Database Server;** - Customer and organisational specific information storage hosts are also both highly sensitive areas that should be treated separately to ensure that no incorrect use of system resources occurs.

- **Application Server; –** There are a number of internal Application Servers that need specific access controls applied. They will need very similar restrictions as the Database Servers, but may need specifics that are best applied through separate Group Policy.

Figure 4 – *The Active Directory Structure*



Example Breakdown of Organisational Units



DNS

The installation of Active Directory requires the presence of a name server as a prerequisite. The DNS is needed because the AD requires more than the simple character strings used as part of the replacement for the NetBios naming system (a NetBios name version is still stored as hosts are added to the system even though they are not required). Resources within the GIAC network are now named in accordance with the Internet naming system. Fully Qualified Domain Names are used for each host. For example one of the Human Resource Application Servers is named ***hrapp1.dm1.generous.com***, while the Domain Controllers in the city centre network are ***dc1.dm1.generous.com*** and ***dc2.dm1.generous.com***.

There is an option for the network to use Dynamic DNS in order to allow remote users to modify their host name and have it automatically registered with the DNS (and DHCP) server. This option was selected as part of the install since this will allow system administrators to alter existing names or add new hosts without needing to add these to the DNS records. The other options that were chosen for the DNS implementation are;

- Restiricted zone transfers – Zone transfers are not required in the GIAC implementation of the DNS. The internal Domain Name Servers will have their configurations shared as part of the AD replication. The external DNS is manually configured.

- Enable “Only Secure Updates” – with this option selected, Kerberos authentication is used to validate each of the updated records. This overrides the default option that would allow any user to change their DNS entry. Secure dynamic updates are only possible in Windows 2000 systems with Active Directory integrated DNS servers.

- Enable logging – security sensitive hosts such as the DNS should always have logging enabled, and these logs should be checked regularly to ensure that the organizations security policy has been applied as expected, and is working correctly. Logging can include such activities as; Queries, Updates, Notifications messages, the number of DNS query messages received, and a number of other useful items.

- Enable the “Secure cache against pollution” option – this was configured on the DNS to protect it against overloads due to the system having to handle a large number of unnecessary or malicious requests (Fox, 2002)

It is worthwhile having a backup DNS in each network for redundancy. Since the GIAC organization has a limited budget, the internal DNS in the R&D network will act as the backup for the city centre network and vice versa. This would normally require trusts to be explicitly configured, and for zone transfers to be permitted between these hosts. However, since the Domain Name Servers reside on the Domain Controllers in an homogenous Windows 2000

design, the automatic replication of Active Directory will keep the Domain Name Servers in a acceptable level of synchronicity.

Replication

The Active Directory structure within the GIAC network will comprise five separate implementations. Domain controllers will be commissioned, four at the central office (two for ***dm1.generous.com***, and two for ***generous.com***), and one at the Research and Development site (also part of the ***dm1.generous.com*** domain). Since the organisation consists of more than a single domain, a Domain Controller situated in each domain has been configured as Global Catalogue Server so that the complete Active Directory does not need to be replicated between domains. Thus, two Domain Controllers at the city centre site are GC Servers, one in the ***dm1.generous.com*** domain, and one in the ***generous.com*** domain. Any future child domains will also need this feature of Active Directory replication.

The design utilises an IPSec VPN (a reliable connection for the purpose of this design) as the means of connecting the two sites. It was decided that a full Active Directory schema would reside on the remote DC so that the site could run independently if necessary. The second DC at the central office will be used in a load sharing role and thus a DC will always be available to the network.

Replication of Domain Controllers requires Kerberos authentication. The Kerberos authentication service is essential to the GIAC organization since it is used for all internal network access and communications. If the organization had legacy NT networks, then NTLM authentication would also be needed, but since the network design relies totally on Windows 2000, then Kerberos v5 will be used throughout (NTLMv2 is still added to the athentication configurations in case a host cannot use Kerberos for some reason). Thus, the Domain Controller also acts as the Key Distribution Centre, which in turn utilises the Active Directory as its database (Schmidt, 2000).

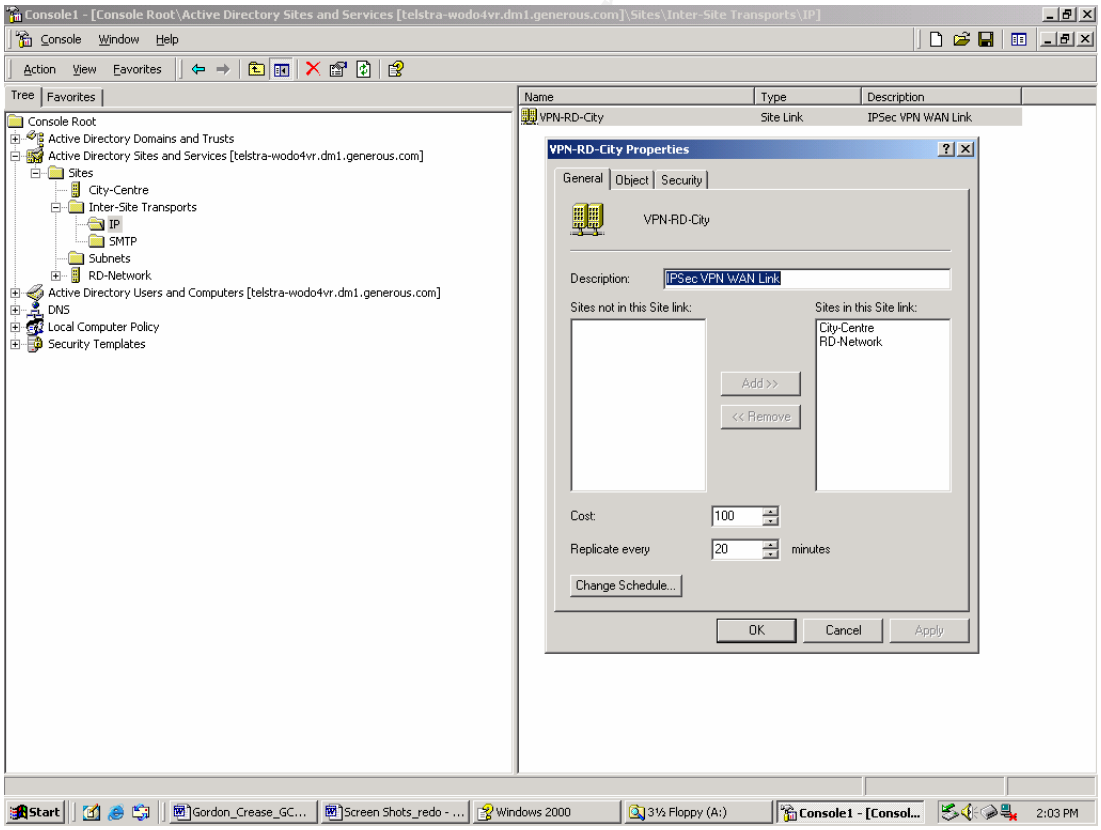
As part of the configuration stage it was necessary to register the two sites that make up the GIAC system. The Domain Controllers in the city centre network replicate automatically via the Knowledge Consistency Checker (Schmidt,2000), but the remote DC in the R&D network was ***linked*** via the ***AD Sites and Services Snap-in***. Two sites were configured, the RD-Remote and the City-Local. The IP Inter-site Transport link was configured for the RPC replication, with the default time of every 20 minutes set. Once the sites have been running satisfactorily for a period, this time setting may be reviewed.

The contents of the Domain Controller Active Directory at the central office will be replicated entirely. The VPN connecting the central office with the remote site will be continuously in place and replication using RPC over IP will be set to take place on a regular basis. This is the only sensible option for the GIAC organisation since replication using SMTP is not available within a single domain and is only used where several domains make up a network

connected via probably slow, unreliable WAN links (Sanderson, 2000). Again, simplicity is a prime key in setting security requirements. Replication of the DC using RPC over IP also means that the IIS SMTP service does not have to be installed on the DC (a service that could possibly have been exploited by an attacker) and an internal Certificate Authority does not need to be set-up to provide PKI services for encryption of the SMTP replication traffic (Schmidt, 2000).

The RPC traffic replicates over the NetLogon secure channel. Therefore as part of the Domain Controller install process, Global Policy will be used to ensure that the channel is secure and suitable key management is used (see Global policy & security in later sections). Replication uses time stamps, Update Sequence Numbers (USN's) and Global Unique Identifiers (GUIDs) to ensure that conflicts that can occur are resolved and that only new information is replicated.

Figure 5 – *WAN Link Settings for Replication*



FSMO Roles

The Flexible Single Master Operation (FSMO) master server operations on the Domain Controllers within the forest have to be determined. This type of Master Server management is used if Multimaster Replication is not suitable which is the case with the GIAC organization, which has more than a single domain.

By default, all five Masters would have been placed on the ***generous.com*** DC upon promotion since it is the root domain. However, there will also need to be a RID Master, Infrastructure Master and PDC Emulator in each domain. There is only a need for one Schema Master and one Domain Naming Master in the enterprise.

The ***dm1.generous.com*** also needs these three Masters placed on a Domain Controller within its domain. Since there are two DCs in the ***dm1.generous.com*** domain, the RID and PDC master will be placed on one, along with the Global Catalogue Server, and the Infrastructure Master will be placed on the second DC since it is recommended that this Master not be on a host that is also a Global Catalogue Server.

The RID, PDC and Infrastructure master placed on the ***generous.com*** DC by default will be moved to the other DC in that domain. The Global Catalogue server remains on the DC that hosts the Domain Naming Master (Fossen, 2002).

Note: Although the GIAC organization is a complete Windows 2000 design, the PDC Master also serves as the authoritative time source for the domain as well as the default server for the editing of Group Policy (Rosenfeld, August 2000).

Installation of Active Directory.

The GIAC organisation is running a strictly Windows 2000 configuration. Due to this design, the Domain Controllers have been implemented to run in Native Mode. This provides the administrators with the opportunity of using all the new security functions that the Windows 2000 operating system offers over its predecessors.

There is no requirement in the GIAC network for merging a legacy NT domain into the design. Some of the important features of native mode are; the support for password filtering on Domain Controllers, Nested Groups and Universal Groups. A particularly important feature of running the DCs in native mode is the ability to turn off the use of NetBios over TCP/IP. The Windows 2000 GIAC network will use SMB but will no longer require NetBios or Wins (Windows 2000 uses DNS to resolve host names). Throughout the network, router and firewall rules can be set to permit the operation of SMB over port 445 rather than 139. This configuration reduces some, but not all of the risks

associated with running NetBios. (By disabling port 139, Null user session attacks can be avoided) (Schmidt, 2000).

The Active Directory installation process starts with the administrator running ***dcpromo.exe*** at the <Run> line of the server being converted to a Domain Controller (note that a Domain Controller should be fully patched with the latest available version before promotion takes place).

The ***generous.com*** root domain was firstly configured, and then the ***dm1.generous.com*** DCs were promoted. The choices for the ***dm1.generous.com*** DC promotion are shown below, indicating the requirement for the inclusion of a child domain.

The options chosen for GIAC were;

- "Domain Controller for a new Domain"- since this is the first server to be promoted, this selection allows for the Domain Controller to be configured to be the first DC in the domain

- "Create a new child domain in an existing domain" – the domain ***dm1.generous.com*** is new and will be a child of the root domain

- "Create this new domain tree in an existing forest" – this is the first domain that will be added to the root domain, which exists in its own forest. This selection has more importance when promoting a second (or any subsequent) Domain Controller as it determines if a new AD schema is created.

- "Permissions only compatible with Windows 2000 server" – GIAC is being constructed as a complete Windows 2000 domain. This option avoids the pre-Windows 2000 permissions that will allow anonymous users over the Internet to read Active Directory entries via a null user session.

Once the choice to change to Native mode was selected, it was accepted that this was a one-way process. This choice was acceptable due to the nature of the network architecture (no legacy NT domains). Also as part of the installation of the first Domain Controller, the option of configuring the computer as a Domain Name Server (DNS) will also be selected.

An important option offered during the Active Directory installation is the password used by an administrator to restore the Active Directory database from a backup. The administrator should ensure that they choose a 'strong' password that is not readily shared (Rick, 2002).

Additional Security Concerns

Upon completion of the Domain Controller promotion of the Windows 2000 server, it is essential to make a backup to ensure that if a disaster should befall the system, it can be quickly restored to its former configuration.

There are many details that should be considered when making backups of critical network systems. They should be considered as a small part of a complete Disaster Recovery plan that should take into account how often backups are produced, what storage medium should be used, where and how will the backups be securely stored, who should have access, and most importantly, how often should restorations be checked. The processes should be carefully checked and documented. If a site is hosted by a professional hosting company (such as the case with the GIAC organisation), there is often the possibility to take advantage of a backup service which will take any media used off-site to a secure location.

An important but often overlooked security requirement for a Domain Controller is the limiting of physical access to any host that is being use to support Active Directory Services. It is generally accepted that the host should be logically secured so that access to the services are restricted using suitable credentials. However, it is equally important that any DC be securely closeted to limit access to the console. The GIAC organization has locked rooms that are only accessible to the two system administrators. Firewalls and critical network nodes are also kept secure in the same manner. Network nodes such as router and switches are as important to system security as are the hosts supporting critical systems. Physical access to these should be no less secure.

Auditing of any failed access to the \NTDS and \SYSVOL folders and their files has been configured so that the system administrators can monitor any network misconfigurations and be warned if unauthorised access is being attempted from within the GIAC organisation.

Group Policy and Security

Introduction

Group Policy is the mechanism developed for the Windows 2000 configuration that allows system administrators to set security policy over the range of the enterprise from a centralised point and over a wide range of functions (Haney, 2001). For example, the Group Policy Framework includes;

- Accounts; - the area covering user accounts and the policies that can be applied
- Local Policy; - covers local user rights to individual computers or system resources
- Restricted Groups; - allows the administrator to control access to the more sensitive and potent security groups such as the Administrator Group
- System Services; - permits specific service activation to be controlled
- Registry; - the very sensitive Windows registry keys can have specific policies applied at an individual level
- File Systems; - separate files can be have access policies and usage policies specified
- Public Key Policies and IPSec; - If public keys are used for any reason, such as for setting up IPSec VPN's, policies can be specifically applied, as can the IPSec filtering rules.

In general, Group Policy can be applied to both the user and the computer and to any resources that are used within an enterprise if they are placed within an Organisational Unit. These policies can be developed in house to be extremely specific to the enterprise, or they can be sourced from such sites as Microsoft and the National Security Agency where templates have been developed for particularly high security purposes (the NSA site was particularly useful for a range of Windows 2000 Guidelines that were of prime importance in the writing of this document).

Templates can be downloaded and applied directly or modified to suit the enterprise. The standard Windows 2000 server install also comes with a number of pre-defined policy templates to help the system administrator with Group Policy application. These can be applied directly, or modified, saved and then applied.

The Group Policy Objects used in the GIAC organisation were base on the templates that came with the Windows 2000 install but modified in a manner

that was more in keeping with the a preferred organisational security policy. The templates sourced from the National Security Agency (NSA) site were reviewed, but found to be more severe in the restrictions than required. Those sourced from the NSA site related to;

- The Organisational Domain – the settings suggested by the NSA were highly extreme, as would be expected for a security related department, but were seen as too *strong* for use directly within the GIAC network. For example, password length was suggested to be at least 12 characters. Large passwords that are rotated on a regular basis can cause the general user difficulty and may lead to weakened security as the user may need to have access to a written copy. The GIAC system administrators realised that for general staff usage, smaller passwords would be acceptable and reduce administration overheads for resets etc.

- The Organisational Domain Controller (Note: the ***Domain Controllers*** is a default Organisational Unit that comes with the Windows 2000 install. All DC's within a domain are automatically added to this OU as they are promoted. The Domain Controller Organisational Unit has its own Group Policy applied by default. However, it was accepted by the system administrators that the DCs need high levels of security, and so they applied a modified version of a Windows template that suited the organisation.

- Servers within the Domain – Medium to high security rules were needed and thus only a small number of the NSA suggestions were considered.

- Workstations of users – as with the Servers, only some NSA suggestions were considered. These devices are normally abused by users, so restrictions were applied that limited access to desktop and Start menu functions.

Precedence

One of the most important issues that arises when Group Policy is applied to the separate levels of the Active Directory hierarchy is the precedence of the policy. Normally the order is;

- Local policy
- Site policy
- Domain policy
- Organisational Unit policy
- Child Organisational Unit policy

It is important to be aware of the affects that precedence has on the application of security policy since, for example, policy applied at the local level is overridden by that applied at the Site level and that is overridden by the Domain Policy (Sanderson, 2001).

There is an option to block the affects of precedence, but it is important that system administrators are aware of the conflicts that can occur if this situation is not properly understood. Within the GIAC organisation, the Domain policy has been configured with the minimum acceptable settings for the credential requirements. These are set by the organisational security policy.

Policy will be applied that is more extreme in some cases where the credentials for users need to be stronger than those that have been applied to the domain as a whole. This will occur for access to system configurations such as the Domain Controllers, so that changes to Active Directory or DNS etc will be better protected. More severe security levels may be applied to the credentials of users who wish to access the network remotely, or for any administrator roles associated with their position.

Group Policy Management

Since the staff levels within the GIAC organisation are small, it was decided that two levels of Group Policy administration be permitted via User Groups;

- **Domain Administrator;** This role will have total rights over the Group Policy associated with the OUs at the Domain level (including Domain Controllers). Since this is the highest level in the organisation, the precedence will allow the Administrator to apply security policy at the highest level knowing that it will be applied to all Ous.

- **Local Administrator:** Members of this user group will have access rights to manage the Group Policy Associated with a particular OU such as the Human Resource OU. The roles associated with this type of access may be needed if GIAC grows substantially in the future.

The concept of Precedence allows for the determination of these roles as the Domain Administrator will be able to apply governance rules over the entire organisation by modifying Domain Group Policy to suit the needs determined by changing security policy within the GIAC organisation.

Originally, the users in these groups will consist solely of the two system administrators presently working for GIAC, but later there may be a need to designate other administrators to spread the workload.

Planning

Before trying to apply any form of Group Policy it is worthwhile determining the areas in the organization that should be considered as requiring some form of security policy to be applied. In the GIAC organisation, the system administrators were aware that there are areas that need to be taken into account when determining the security policy. The organisations various Group Policy will need to take into account;

- Workstations; - there are several different types of users within the organization. These relate directly to the organization hierarchy. Fixed workstations for HR and Marketing users were deemed to have similar requirements.

- Printers; - these need to be treated separately as they can be used by malicious users, and have different requirements to their human counterparts

- Users; - There are several types of users who will be matched with the predetermined roles set up for specific types of access to servers, printers, databases etc

- Servers; - Applications servers require different access to the those serving mail, or the DHCP and DNS resident on the Domain Controller.

- Auditing; - it is important to have different types of auditing depending upon the resource type and how it is being used within the organisation. Administrators had to take into account the heavy load that audit logs can place on memory resources.

Domain Policy

This Domain Group Policy template is aimed primarily at managing user credentials for the enterprise and will cover;

- Password Policy
- Lockout Policy
- Kerberos Policy

Note: The default Domain Policy defines the above sections from within Windows Settings/Security Settings/Account Policy tree structure, while the default Domain Controller Policy defines the local settings from within Windows Settings/Security Settings/Local Policies. At installation, settings are predefined in these areas and are worth noting before changing. They may already suit the organisation.

To investigate the existing Domain Policy, via the MMC console, navigate to <Active Directory Users and Computers>. Right click on the domain in question, and select <Group Policy>. The select Edit to see the settings. A new screen will appear that shows the Domain Policy settings and will allow changes to be made.

Figure 6a *– Checking Domain Group Policy*

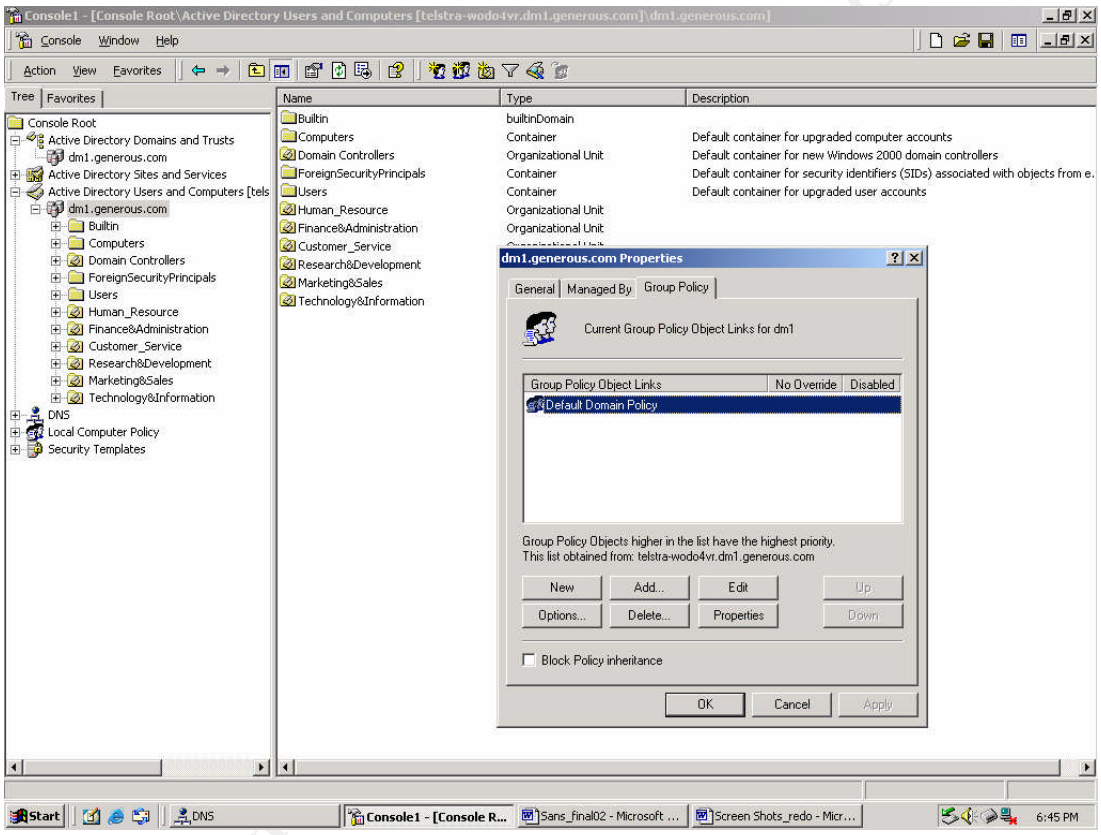
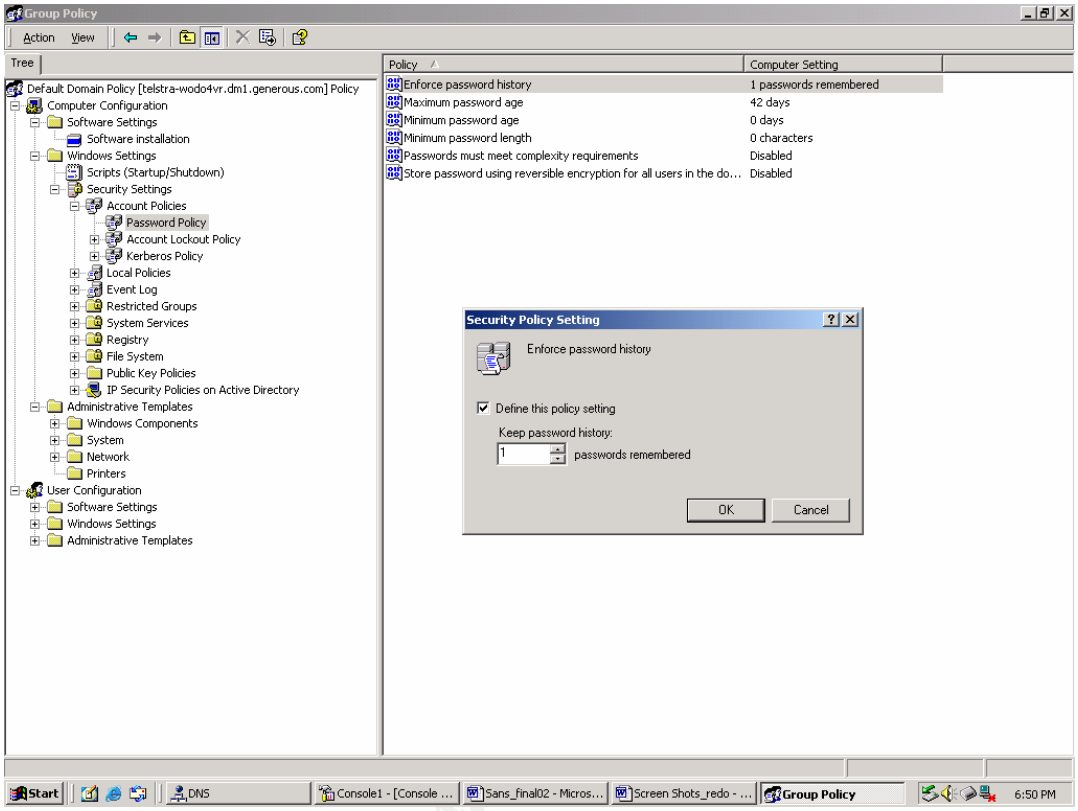


Figure 6b *– Checking Domain Group Policy*



Domain Password Management

Password management is a major security requirement for any organisation and should not be taken too lightly. Suitable choices made in the implementation of this template can let the system administrator develop a user access control model that is built on a solid foundation.

System administrators should be aware of user habits where credential handling is concerned. If there is an attempt to impose a too severe policy, users will find ways to store passwords in unsatisfactory ways. It is important to understand the nature of the organisation and the user requirements when choosing which settings are selected. Since the GIAC organisation is only small in relation to the numbers of staff, the system administrators will be able to more closely monitor credential usage and can have a very direct impact on how each user handles the credentials they are given.

Before applying a new Group Policy to the Domain, it is worth checking the existing policy. This can be done by relatively easily by accessing <Adminstative Tools> through the <Start> Menu, and navigating to <Active Directory Users and Computers>. From here the policies that have been

applied to any OU can be determined by right clicking on the folder and following the Properties link.

The settings for the Domain are as follows;

- **Password Policy**
  - Enforce Password History: 8 passwords remembered - there is no reason to make this value too high as most users will not be able to remember past passwords for any great length of time.
  - Maximum password age: 90 days - approximately 3 months is an accepted default standard.
  - Minimum password age: 1 day - this is useful for providing new passwords to users that need to be changed at first logon.
  - Minimum password length: 8 characters - if a password is too long, users will have difficulty with memory and will need to write it down in a possibly accessible place.
  - Passwords must meet complexity requirements: Enabled - this provides for non dictionary style passwords with the inclusion of alphanumeric characters (much more difficult to crack)
  - Store passwords using reversible encryption for all users in the domain: Disabled.

- **Account Lockout Policy**

  An effective account lockout policy is essential in limiting the opportunities of attackers in simple password guessing exploits.

  - Account lockout duration: 15 minutes - if account lockout is enforced for this time an authorised user will probably make a later attempt rather than requesting help from the administrator, but it is long enough to disuade unauthorised users.
  - Account threshold lockout: 3 invalid logon attempts - a default standard that allows for keyboard errors
  - Reset account lockout counter after: 15 minutes - set to match lockout duration
  - Enforce user login restrictions: Enabled

Within this Group Policy are Kerberos settings that have been configured because the key ticketing system is being used within the GIAC organization for all authentication (except for the IPSec VPN).

- **Kerberos Policy**

  - Enforce User Logon Restrictions – this is enabled and has the affect of requiring every request for access to a service to be checked by the KDC. The user right on any server accessed is checked. This adds overhead to the network, but is deemed acceptable for the Single Sign On across the organization

  - Maximum Lifetime for Service Tickets – the default option of 600 minutes is kept. This will give a ten hour period for a user of the system to access a service, such as a printer.

  - Maximum Lifetime for User Tickets – The 10 hour default is geared to match an extended logon period. If a user is still logged-on at the time limit, a new ticket will be issued by using cached information.

  - Maximum Lifetime for User Ticket Renewal – The value of 7 days means that a renewal will last for a week, but after this period, the user will need to re-authenticate.

  - Maximum tolerance for computer clock synchronisation – A five minute difference in clock values for ticket granting is tolerated.

As stated earlier, the System Administrators noted during the planning stage that auditing is an essential part of any security regime. Therefore, as part of the Domain Group Policy, some of the auditing options were selected. The primary aim of applying auditing policy at the domain level is to check for any successful administrative changes. Similarly, failed attempts are also important since they may indicate attacks (or any unauthorised access attempts) on important system hosts. More detailed auditing requirements have been applied through other Group Policies Objects that have been linked to local systems. The domain auditing requirements are;

- Audit Account Management – (success, failure). Check for any possible changes to account access controls. Attempts might be made to add or delete accounts.

- Audit Object Access – (success, failure). This is important for monitoring any access to the Active Directory Objects themselves.

- Audit Policy Change – (success, failure). Any Policy changes should be logged and checked to ensure no conflicts or errors.

There are several other audit options available to the System Administrators, but these are applied at a lower level of specific Ous. These include the auditing of logon attempts.

Domain Controller Group Policy

Probably the most important hosts within any network are the domain controllers. In a Windows 2000 implementation they take on additional importance as they now support the Active Directory where access security information is stored and managed (Schmidt, 2000). In the GIAC network the hosts on which they reside also support the DHCP server and the Domain Name service for the organisation. These hosts therefore need to be protected above all others.

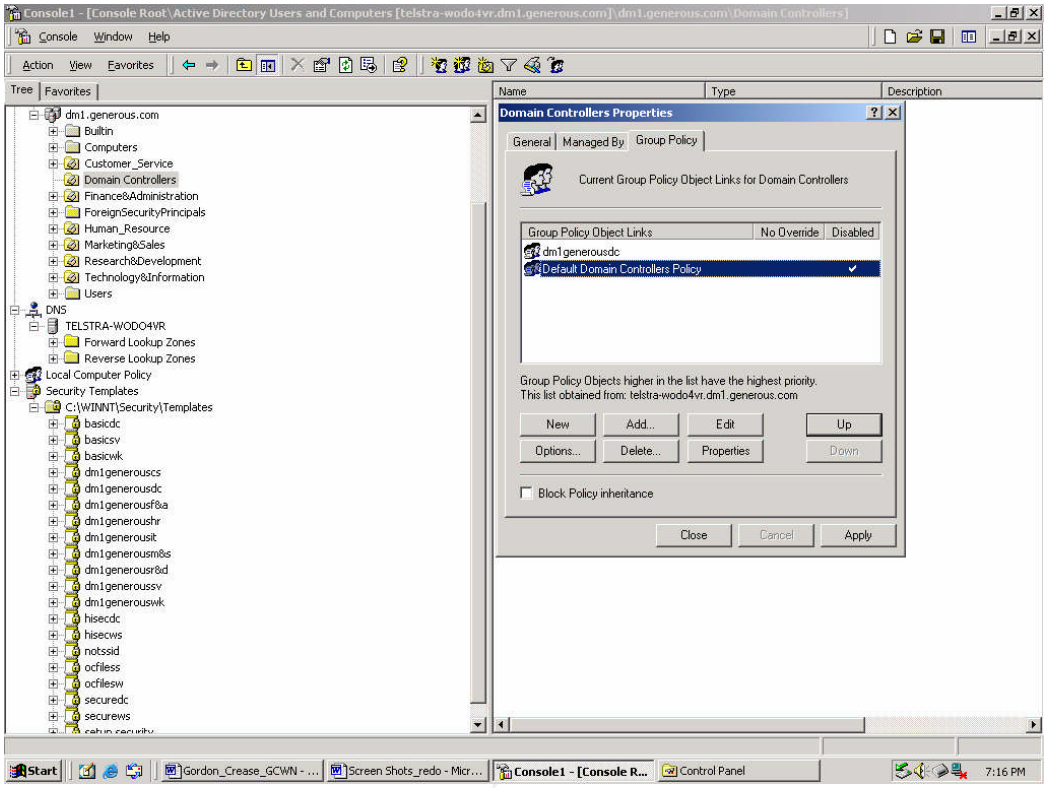
The default Windows 2000 build comes with three Domain Controller Global Policy templates that can provide various levels of security (Windows ratings) of basic to high. The ***basicdc.inf*** template was chosen, modified to suit the organisation, and saved as ***dm1generousdc.inf***. This new Global Policy Object was linked to the Domain Controller Organisational Unit.

There are now two group policies that have been applied to the organisation's Domain Controller OU, but which provide slightly different security functions. The Default Domain Controller Group Policy was left untouched but disabled. The ***dm1generousdc.inf*** policy reflects the DC system administration preferred by GIAC, and covers logging, system services and the file systems etc.

A separation of security functions allows system administrators to make modifications to a particular area without the fear of accidentally affecting another. Thus if a problem were to occur in the GIAC modified DC group policy, it could be disabled and the Default Domain Controller Group Policy quickly and easily applied.

The Group Policy that applies by default to the <Domain Controllers> Organisation Unit can be inspected by navigating to <Active Directory Users and Computers> (using the MMC and associated snap-in). Right click on<Domain Controllers> and check <Properties> and then <Group Policy>. See figure below.

Figure 7 – *The Group Policies applied to Domain Controllers*

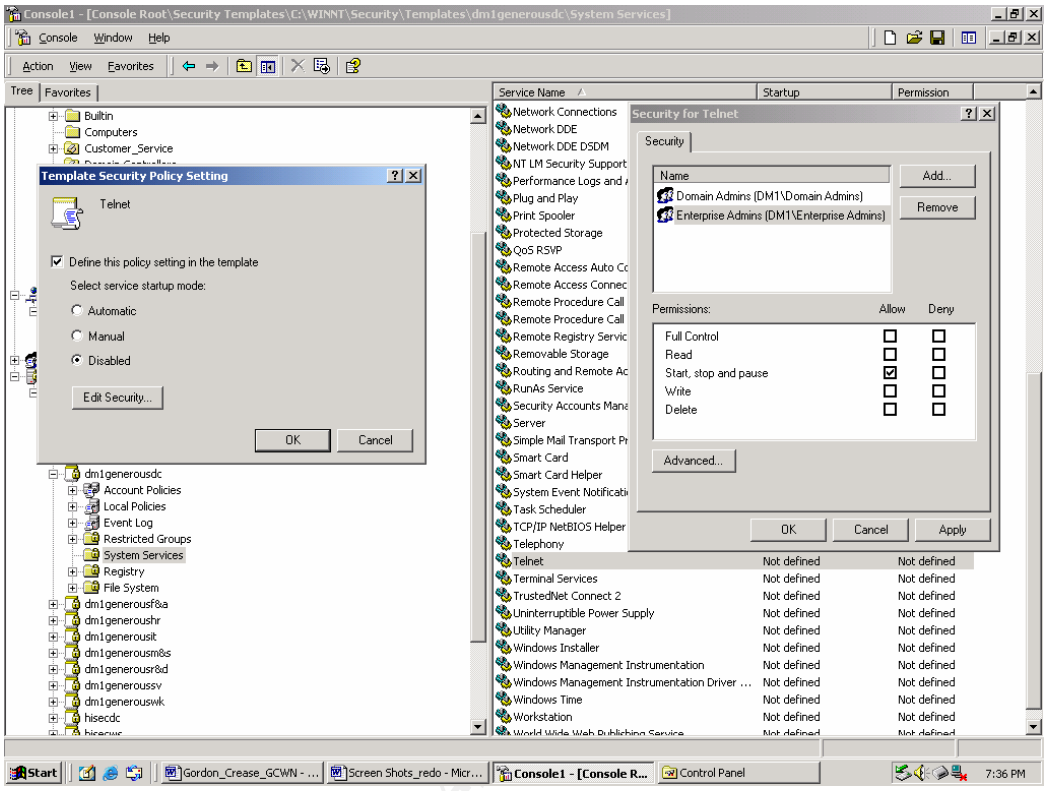


Controlling Services on Domain Controllers

The ***dm1generousdc.inf*** Group Policy will apply a set of preferred options. For example, all system services have the option to be set to run at startup automatically, manually, or disabled. Each service has been stepped through by the GIAC system administrators and any unnecessary services disabled. Similarly, permissions relating to access to each of the services was changed. The ***Everyone*** group was deleted and the ***Domain Administrators*** and ***Enterprise Administrators*** were added.

Management of the services on all Domain Controllers should be accessible only to the Domain Administrators or the Domain Controller administrators (the latter group can be used in large organisations with multiple domains to distribute management privileges – GIAC was deemed to small to require the use of this group directly, but it was added for future use). The two GIAC system administrators were added to both these groups.

Figure 8 *– The configuration of Telnet services on the Domain Controller (An example of service options)*



The aim of disabling many of the services running on a Domain Controller is to ensure that they cannot be exploited by an attacker. If a service is not needed on the host then it should not be listening at boot-up of the system.

Some of the other services that need to be either disabled or configured for manual starting are;

- IIS Admin Service (disabled) – no Web server is being run on any DC in the GIAC organization
- World Wide Web Publishing Service
- Fax Service (disabled) – an unnecessary service for a Domain Controller
- NT LM Security Support Provider (disabled) – NT LM is not being used in the GIAC design
- Simple Mail Transfer Protocol (disabled) – The DC is not being used as either a mail relay or mail server.
- TCP/IP Netbios Helper (disabled) – Netbios is not being used within the GIAC organization since it is has no legacy NT systems
- NetMeeting Remote Desktop Sharing (disabled) – any service that is specifically user related is not necessary on an enterprise controller or server

- Plug and Play (disabled) – this is an unnecessary service and has been known to have vulnerabilities
- Smart Card and Smart Card Helper (disabled) – this service could possibly used in future implementations of authentication in GIAC, but is not necessary originally

Logging of Actions on the Domain Controller

Domain Controllers need a high level of security applied at all levels. An important area of security is in the logging of actions such as access attempts (either failed or successful). Settings have been set that are more severe than for other computers within the organization. The ***dm1generousdc.inf*** policy covers Even Log settings and those chosen for the GIAC organisation are;

- Maximum application log size – 50 MB. This size was chosen as large enough to allow the system to collect information for at least two weeks (hopefully). As with all log size choices, it is a matter of trial an error. Once they have been set up on the organisational controllers and servers, it will be necessary to 'fine tune' the sizes to suit the administrators. Regular checking and archiving will allow for smaller sized logs, but often, logs are not checked until a problem occurs and forensic information is required.

- Maximum security log size – 100 MB. Large enough to collect all the necessary information for forensic investigations of user accesses for four weeks (hopefully).

- Maximum system log size – 35 MB

- Restrict guest access to application log – Enabled. This and the following two selections were disabled even though access to the Domain Controller is limited to Domain Administrators via the group policy. Safety when setting access is to deny permission unless there is an understanding of the affects.

- Restrict guest access to application log – Enabled

- Restrict guest access to system log – Enabled

- Retain application log – Overwrites events older than 14 days. This and the following two sections cover the length of time the logs will be kept before they are overwritten. Logs relating to security sensitive hosts such as Domain Controllers should be viewed daily if possible. However, the role of system administrator does not always allow for such strict scrutiny. Longer period of log retention also allows for analysis of possible long term unauthorised attacks. These settings may need to be reviewed after the GIAC organization has been operating for a short time.

- Retain security log – Overwrites events older than 28 days.
- Retain system log – Overwrites events older than 14 days
- Retention method for application log – Overwrite events as needed
- Retention method for security log – Overwrite logs as needed
- Retention method for system log – Overwrite events as needed
- Shut down the computer when the security audit log is full – Disabled. It would not be sensible for any Domain Controller to be automatically shut down during normal daily operations.

Note: There are risks associated with allowing logs to be automatically overwritten. The process allows a possible attacker to cover their tracks if they manage to compromise a host. However, until the GIAC administrators have an understanding of the log sizes that will eventually be generated, as well as inspection and archiving policies, the logs will be overwritten.

Additional Group Policy

Apart from setting group policy for the domain controllers and for the organisational domain itself, the GIAC system administrators also set Group Policy to cover each of the Organisational Units that make up the design of the Active Directory. These additional policies were added as a protective measure and mirrored the policies in the Workstation Group Policies, as well as Server Policies. They were linked to their associated OU, but disabled, only to be used in case problems with the preferred Group Policy is experienced. They can be enabled and applied quickly if necessary, and will provide security for the computers in an OU while the administrators work on the preferred Policy.

For example, the ***dm1generoushr.inf*** is linked to the Human Resource Organisational Unit, and the ***dm1generousr&d.inf*** is linked to the Resource and Development OU. All the new Group Policy files were stored in the %system%\security\templates directory (see Figure 7 above)

The Domain Group Policy settings were designed to set the minimum access controls that would be permitted within the organisation, along with basic audit policy. Precedence will apply and so the Domain Group Policy will dictate the specified settings relating to Password Access and some Auditing. The additional group policies were then aimed at either applying rules to specific systems, or to allow particular actions to be taken at the local level.

Although the GIAC organisation is separated logically into several business units, such as Human Resource, Finance and Administration etc, it was seen to be acceptable that users in each unit have identical restrictions placed on the workstations and database servers at this point in time. The security policies may need to be made more granular and more specific to individual users in the future. However, for ease of administration a single set of policies was derived and applied. Close monitoring of user needs will determine any required changes.

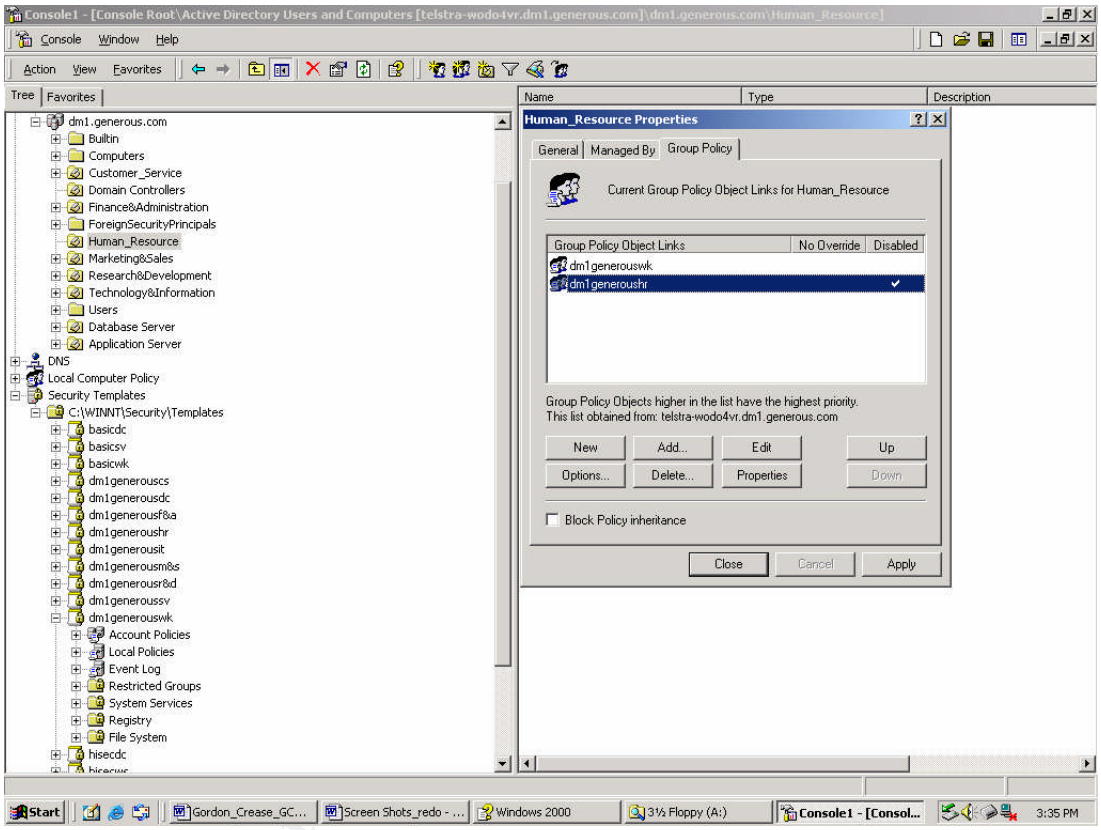
Additional group policies that come with the Windows 2000 install relate to workstations and servers. As with the domain controller templates, the workstation and server templates have three ratings, basic, secure and high. Since the GIAC organization is still relatively small, it was decided that a single workstation policy could be linked to each of the Organisational Units. However, once the template was determined, it was renamed for each of the OUs so that they could be modified independently in the future.

Workstation policy

The ***basicwk.inf*** template was selected and modified to reflect the organisational security policy. It was then saved in several formats, one of which is the ***dm1generouswk.inf***. This was linked to the Human Resource

Organisational Unit by navigating to the Human Resource Properties screen and selecting <Add>. See figure below which shows the workstation policy link and also the OU specific group policy mentioned earlier, which is disabled.

Figure 9 *– The application of a workstation group policy*



Workstation group policy in GIAC was designed to cover the security settings on the local user machines. The <Security Options> was selected in the policy object, and the followings settings were set;

- Amount of idle time required before disconnecting session – 30 minutes. This time refers to the continuous idle time in a SMB session and should not be confused with the screen saver idle time. The default value was chosen as acceptable.

- LAN Manager Authentication level – NTLMv2. responses only/refuse LM.

- Prompt user to change password before expiration – 3 days. It is worth prompting users so that they will have time to select a suitable

password. It is important, however, that the user not be tormented by the process.

- Clear virtual memory pagefile when system shuts down – enabled. Pagefiles can cause system problems both in usage and security, and should therefore be cleared during the normal shut-down process. Possibly corrupted data will then be purged nightly, or at each normal shutdown of the system. However, this process can take several minutes to complete and therefore should be monitored to see if it is adversely affecting users.

- Audit the Access of Global System Objects – Disabled. Workstation auditing would be an unnecessary use of local resources since it is doubtful the GIAC administrators would need to (or have the time to) check local workstation logs.

- Audit the Use of Backup and Restore Privileges – Disabled. As above

- Do not display last user name in logon screen – Enabled. This ensures that users must be able to identify themselves as well as providing a password. Displaying last user name aids in a localised password guessing attack and allows for the collection of UserIDs.

- Disable CTRL+ALT+DEL Requirement for Logon – Enabled.

- Number of previous logons in cache (in case domain controller is not available) - 1logon. Workstations are allocated to single users and therefore only that user should have their credentials cached. Domain Controllers in the GIAC organization have been designed for redundancy, and therefore should be available.

- Prevent users from installing printer drivers – Disabled. Users should be able to install printer drivers from over the network.

- Smart Card Removal Behaviour – Not Defined. Smart Cards are not yet a part of the GIAC authentication process.

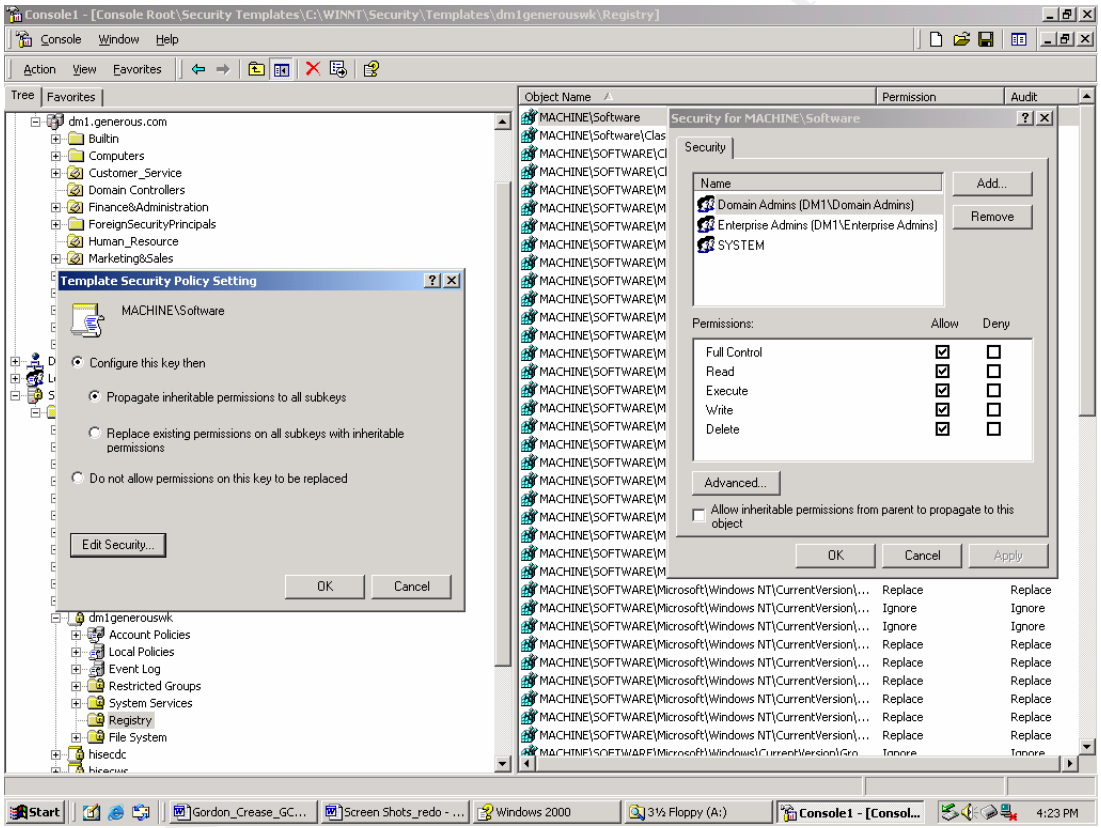
The points mentioned above are some of the options set for GIAC that relate directly to workstation users. Although there are many more settings that relate to items such as Internet Explorer, and Windows specific updates etc (which are disabled), they do provide an indication of the level of control that can be placed on individual workstations. Other options include settings for local media use and secure channel selection.

Another important set of policies that need to be applied to a workstation relate to the access controls being placed on the Windows Operating System files. This is one of the more complex processes for the system administrator, but it is worth taking the time to step through each of the files and at least controlling user access to those only specifically needed for normal business functions. Dynamic linked library files and executables for example should not

be able to be modified by a general user. Care must be taken to ensure that the system operation is not compromised.

In the Group Policy it is important to make sure that System Files and Registry are not accessible to the general user. The permissions were changed on each Registry Object so that only the GIAC Administrators could have full control. The SYSTEM group was left so that any application that may access the registry as part of its processes could do so.

Figure 10 – *Controlling Access to the Registry*

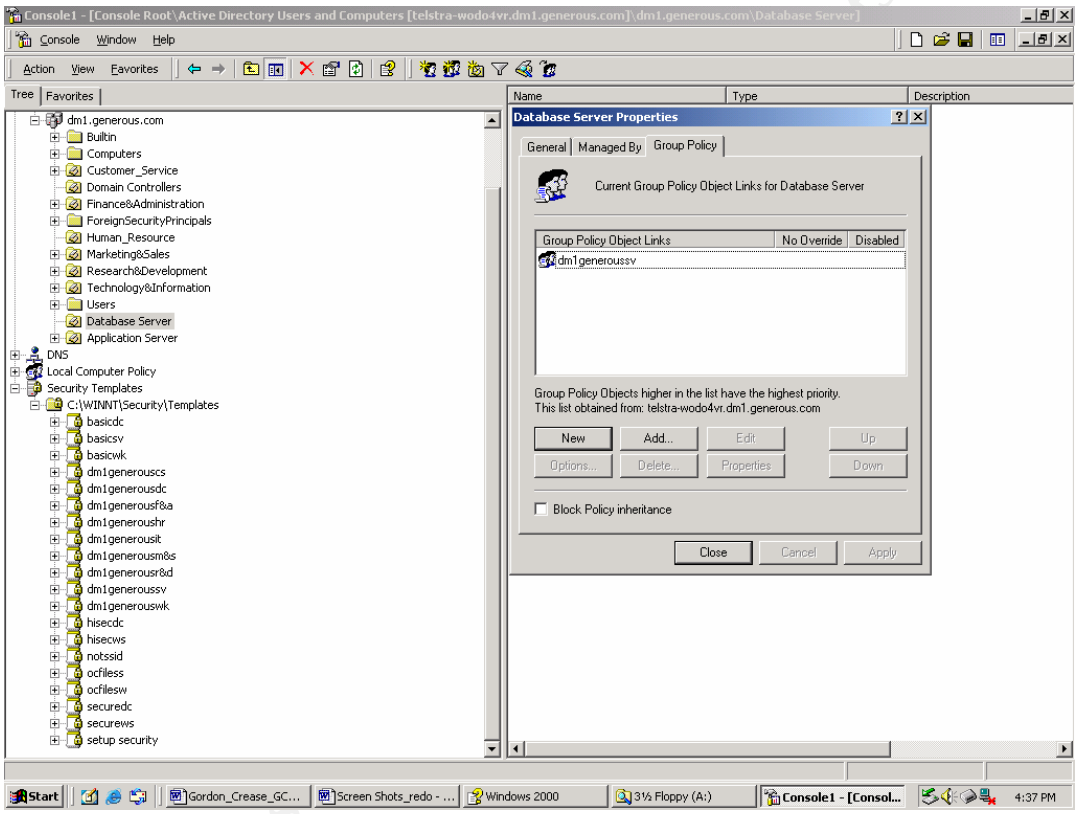


Database and server policy

Probably of equal sensitivity to the Domain Controllers, in relation to security, is the Database Server. There are several of these within the GIAC organization. One is designated for the HR department, another for the Finance department, and a third in the remote office for storage of R&D specific information. These need particular access and security settings that differ greatly from and workstations.

As with the workstation policy requirements, a basic template ***basicsv.inf*** was selected and modified and then saved as ***dm1generoussv.inf*** to be applied to each of the Database Servers in the organisation via the Database Server Organisational Unit. See figure below.

Figure 11 *– Application of the Database Server Group Policy Object*



The policy applied to the database servers is designed to cover the system file access and auditing. It is expected that administration of the database servers will be passed to other GIAC staff members who have database specific training. Thus, it is important for the domain system administrators that controls be placed on access to the Operating System.

The advantage the GIAC administrators have in the application of Group Policy is that precedence will apply to both workstations and the database servers. The Domain Policy will have precedence and so the Administrators will be able to ensure that as long as that Group Policy is properly administered, a minimum level of control can be placed on both these hosts.

Some of the policies applied to database servers in the GIAC organisation are listed below. They are the same as those applied to the Domain Controller since the security of the database servers is considered as critical.

- Audit Account Logon – Success, Failure.
- Audit Account Management – Success, Failure. Keep a record of changes to Group Policy, User Accounts and Passwords
- Audit Directory Services – Success,Failure. This is more important to have set for Domain Controllers.
- Audit Logon Events – Success, Failure.
- Audit Object Acess – Success, Failure.
- Audit Policy Change – Success, Failure. A good audit policy to ensure that user rights or audit policies have been modified.
- Audit Privilege Use – Success, Failure.
- Audit Process Tracking – No Auditing Required.
- Audit System Events – Success, Failure. The administrators can keep a track of restarts of the local machine.

Some of the other policies that have been applied to GIAC servers via the ***dm1generoussv.inf*** Group Policy affect User Rights;

- Disable *Access From the Network*. Make sure that Administrators must have physical access to the server to make modifications.
- *Logon Locally* should be enabled for GIAC Administrators only
- Disable *Add Workstations to the Domain*. This will stop users from promoting the server to a Domain Controller.
- Ensure that only the GIAC Administrators can *Backup Files and Directories*. This setting, along with the following setting, will give GIAC Administrators the ability to backup and restore the database servers. Database Administrators will also have this permission in the future.
- Ensure that only GIAC Administrators can *Restore Files and Directories*.
- Ensure that only GIAC Administrators can *Change the System Time*. This is important to ensure that audit trails cannot be destroyed by malicious users. Also, Kerberos authentication can be compromised by misuse.
- Ensure that only GIAC Administrators can Manage Audit and Security Log. Once again, it is important that logs be free from change by a malicious user.
- Make sure that no user can *Create a Token Object*.
- Do not allow Users to Load and Unload Device Drivers. This would have the potential for a Trojan driver to be loaded by a malicious, or unsuspecting user.
- Only GIAC Administrators will have the ability to *Take Ownership of files or Other Objects*.
- Do not permit *Server Operators to Schedule Tasks*. This is only permitted for GIAC Administrators on Domain Controllers.
- Leave the default setting for Windows 2000 that has *Allow System to be Shut Down Without Having to Log On* disabled. This setting stops a local user to shutdown the system by using the CTRL+ALT+DEL combination.

The context settings above have been gleaned from the *Securing Windows 2000 SANS Step by Step* document, and were considered acceptable for the GIAC organisation.

Another document produced by SANS, the *Windows 2000 Security Standards*, also presents several issues regarding good security practices. Some of these were also adopted. Those specifically selected for Database Servers in the GIAC organisation are;

- Disabling the Guest Account – to ensure that no anonymous access could be gained on any of the servers
- Ensuring that Auditing is enabled for sensitive files and folders – this is particularly important for database servers since they have sensitive customer and/or corporate information.
- Access to sensitive files and folders is restricted – this mirrors the importance of the above item and shows that the GIAC Administrators are aware of the importance of the information stored in the three databases. It is important to explicitly allow specific User Groups access and to ensure that NTFS permissions are also set.
- All activities on the Registry Keys is audited – this should include successful and failed attempts, and the logs should be reviewed as regularly as possible.

Additional Security

A Windows 2000 implementation across an organisation, or as part of an existing implementation can give system administrators the capacity to apply, monitor and manage security on all domain hosts from a central location. This control can be placed over the entire domain through one or several policy objects, or at the local computer level. The application of Group Policy, if effectively planned and managed, can assist the savvy administrator make a network that is efficient and secure. However, there are limitations, and a network can be made more secure through other implementations.

Physical Security

Many attacks on network information or resources can come from opportunist use of unprotected systems. A section of any organisational security policy should be directed towards the physical requirements to be placed on users, hosts and network nodes. The types of controls that can be put in place are;

- Users should have some form of identification that can be used for building and/or room access. In extremely high security areas,

biometrics can be used. However, these are not recommended for normal organisational use as they come with their own management issues.

- Network nodes should be locked in spaces separate from user workstations. Access should be limited to authorised administrators. Secure racks can also be used to further limit access if necessary.

- All users should be made aware of the need for vigilance and be willing to question the actions of any stranger within the vicinity of any host or network resource.

- Users should be instructed in the need for password management. Social engineering of user credentials is quite often a very simple matter. Similarly a hard copy of a password may be stored in obvious and accessible places near a workstation.

- Backup or Archive media should be protected by being stored in a secure location, preferably remote to the host network.

Router and Firewall configurations

There are a great many definitive guides to securing the network perimeter by means of suitable rulesets and access control lists. For example, the SANS organisation provides a list of some basic rules that can be applied and which will immediately improve network security. Some of the basic settings are;

- Configure the border router to deny any TCP packets that have ***spoofed*** IP addresses. This is a simple process and involves a small access control list with perhaps five or six lines.

- Use of unencrypted community strings on devices that use SNMP as part of the management and monitoring process can be dangerous. Disable SNMP whenever possible.

- Ensure that all unnecessary services are turned off, and that patches or hot fixes are applied as soon as possible.

- Use ICMP under controlled conditions. Do not enable all ICMP, but select what is needed for administration. For example, use echo requests and replies on egress and ingress respectively, and drop all other ICMP packets at the firewall. ICMP ping is used by several scanning tools, or as part of a denial of service attack.

- Ensure that ***small services*** are disabled at the border router. Services such as ***chargen*** have known vulnerabilities, and are no longer necessary in a modern network.

Host hardening & patching

There are many unnecessary services that run by default in many installations of Windows operating systems. This problem has been addressed by the versions of Windows that have been developed after NT4. However, even the Windows 2000 Server or Professional implementations can be hardened. There are a number of sites that provide documentation that the astute system administrator can follow to improve security from the default level. But this will come to nothing if Service Packs, hot fixes or patches are not applied as soon as possible.

Any install of Windows 2000 should immediately be followed by the latest service pack (SP 2a at the writing of this document). Subsequent hot fixes and patches should be applied as soon as they are published. However, there is a caveat associated with this last statement. There have been occasions when patches can actually upset system operation, or can themselves produce an unforseen vulnerability. It is still considered to patch rather than not. Regular monitoring of security sites is always recommended.

Auditing

As a regular process, a network should be audited by the administrators, or by an external company, to ensure that organisational security policy is being followed. External scans of the Internet facing systems will provide an indication of the effectiveness of the border router and primary firewall rules. Internal scans of all systems can provide and indication of the build types and patching levels. Unnecessary services can be pinpointed and dealt with.

There are many commercial and freeware tools available, such as Nmap, ISS scanner, that can quickly and easily be adopted to help identify security weaknesses.

References

Jason Fossen, ***Windows 2000: IPSec and VPNs***, version 5.3, September 2002, The SANS Institute, www.sans.org)

Jason Fossen, ***Active Directory, DNS and Group Policy***, version 5.3, September 2002, The SANS Institute, www.sans.org)

Jeff Schmidt, ***Microsoft Windows 2000 Security Handbook***, August 2000, Que Corporation

Symantec Article, ***Security Response; Defense in Depth***, Symantec USA, 2002 http://securityresponse.symantec.com/avcenter/security/Content/security.articles/defense.in.depth.html

Mark J. Sanderson, ***Guide to Securing Microsoft Windows 2000 Active Directory***, version 1.0 December 2000, System Network Attack Centre (SNAC), National Security Agency, http://nsa2.www.conxion.com/win2k/download.htm

Julie M. Haney, ***Guide to Securing Microsoft Windows 2000 Group Policy***, version 1.1 September 2001, System Network Attack Centre (SNAC), National Security Agency, http://nsa2.www.conxion.com/win2k/download.htm

Microsoft Whitepaper***, Introduction to Windows 2000 Group Policy,*** May 1999, http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolicyintro.asp

Microsoft Article, Making Microsoft Servers Secure: Your step-by-step checklist for securing Microsoft Servers, September 2002 http://www.microsoft.com/education/?ID=ServerSecurity

Anonymous, The 60 Minute Network Security Guide (First Steps Towards a Secure Network Environment), version 1.0, October 2001, Systems Network Attack Centre (SNAC), National Security Agency, http://nsa2.www.conxion.com/win2k/download.htm

Paul F. Bartock, ***Microsoft Windows 2000 Network Architecture Guide***, version 1.0, April 2001, Systems Network Attack Centre (SNAC), National Security Agency, http://nsa2.www.conxion.com/win2k/download.htm

Alistar G. Lowe-Norris, ***Windows 2000 Active Directory: Help for Administrators***, O'Reilly, December 200, http://www.oreilly.com

Keith E. Strassberg, ***Firewalls:The Complete Reference***, Berkeley, California, USA: McGraw-Hill, 2002.

Gregory Rick, ***GIAC Enterprise Windows 2000 and Active Directory Design,*** Securing Windows Practical Assignment***,*** Version 3.0, Option 1, May 2002

Trent Fox, ***Implementation of a Secure Windows 2000 Infrastructure at GIAC Enterprises***, GIAC GCNT Practical, version 3, Option 1, May 2002

Gary Rosenfeld, ***Win2K Operation Masters***, Windows & .net Magazine, August, 2000, http://www.winnctmag.com/Articles/Index.cfm?ArticleID=9045

SANS Institute, Editor Jeff Shawgo, ***Securing Windows 2000, Preliminary Edition, Step by Step***, version 1.0a, May 8, 2001

Hilel January, ***Windows 2000 Security Standards***, SANS Institute, Maryland, Columbia April 5, 2001

The Centre for Internet Security, Editor Jeff Shawgo, ***Windows 2000 Professional Operating System Benchmark, Consensus Baseline Security Settings***, Version 1.0, July 17, 2002, http://www.cisecurity.org

Microsoft Corporation, ***Prescriptive Guidance, Security Operations Guide for Windows 2000 Server***, 2002