Global Information Assurance Certification Paper

Group Policies for GIAC Enterprises

Rick Smith
GIAC Securing Windows 2000 Practical (Version 3.0)

Introduction

This paper will discuss some of the security aspects of a Microsoft Windows 2000 deployment in a fictitious small-to-medium sized company. The paper fulfills the practical requirement for the Securing Windows certification of the Global Information Assurance Certification program. The practical requires the design and implementation of a secure Windows 2000 network for GIAC Enterprise, a company that deals in the online sales of fortune cookie sayings.

The GIAC Enterprises corporate structure description

A small-to-medium sized company of 125-150 employees total. The corporation has two locations: Annapolis, MD and San Francisco, CA. The corporate headquarters is in Annapolis. The Headquarters is primarily corporate executives and Marketing and Sales (M&S). The San Francisco site is primarily devoted to research and development (R&D). Both locations have personnel contingents from the Finance and Human Resources (F&HR) and the Information Technology (IT) divisions.

There are five major groups or types of network users: executives, M&S, F&HR, R&D, and IT.

- Executives have desktop workstations and a few have laptops for corporate travel between the two locations.
- M&S personnel have laptops with docking stations that as their sole corporate computer. These personnel carry sensitive corporate sales and contract data on their laptops.
- R&D personnel have desktop workstations. They work on corporate confidential data that is required to be stored on a network drive on a server.
- F&HR personnel have desktop workstations that handle sensitive data on personnel and the corporate finances
- IT personnel are split into three groups:
  - Help desk personnel are responsible for interfacing with the corporate users and printers.
  - Server administrators are responsible for all corporate servers except the domain controllers and servers used for routing.
  - Network administrators are responsible for the domain controllers, servers used for routing, firewalls and all other network infrastructure.

- Each person in the IT department has a normal unprivileged user account for their normal access to the network. In addition, the IT personnel have an additional account that has elevated privileges to conduct their administrative functions.

The GIAC Enterprises intranet is completely Windows 2000 based including servers, workstations, and laptops. All software on the network is Windows 2000 certified.

Network Design and Diagram

The GIAC Enterprises network has two locations, the headquarters in Annapolis and the San Francisco offices. Each location has a T1 connection to the Internet provided by a local ISP. Both sites have corporate routers at the Internet connection with packet filtering capability that act as the exterior firewall. Inside in the corporate router at the Headquarters location, there are three servers connected to the Demilitarized Zone (DMZ): a web server (www.giac-ent.com), a SMTP server (smtp.giac-ent.com), and an Internet Security and Acceleration (ISA) Server. The ISA Server is dual-homed and acts as the interior firewall between the DMZ and the intranet.

The overall network layout is shown in Figure 1. Additional details of the Annapolis and San Francisco sites are shown in Figure 2 and 3, respectively.

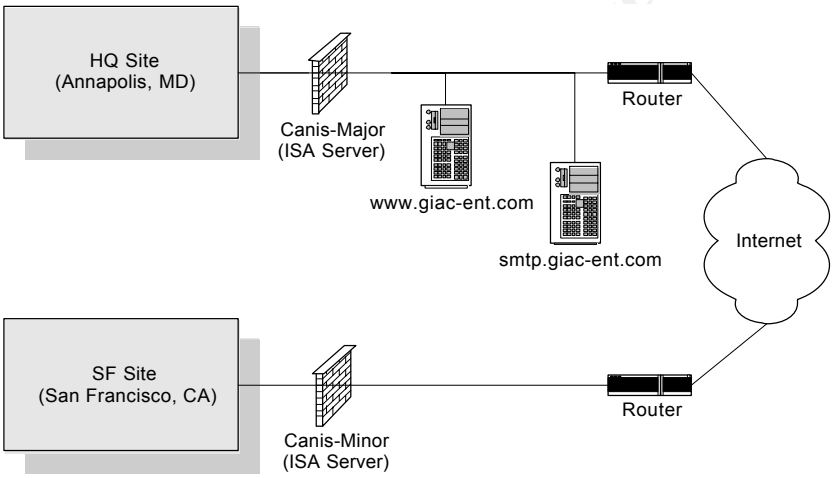

Figure 1, GIAC Enterprises Overall Network Layout

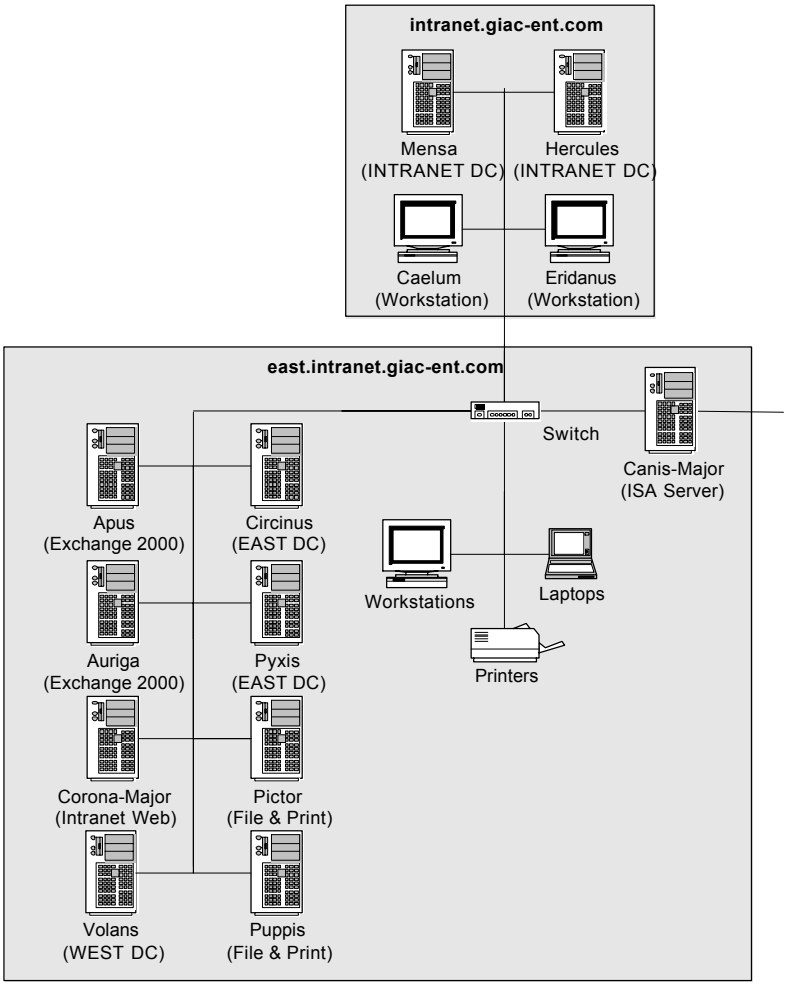

Figure 2, Annapolis Intranet Diagram

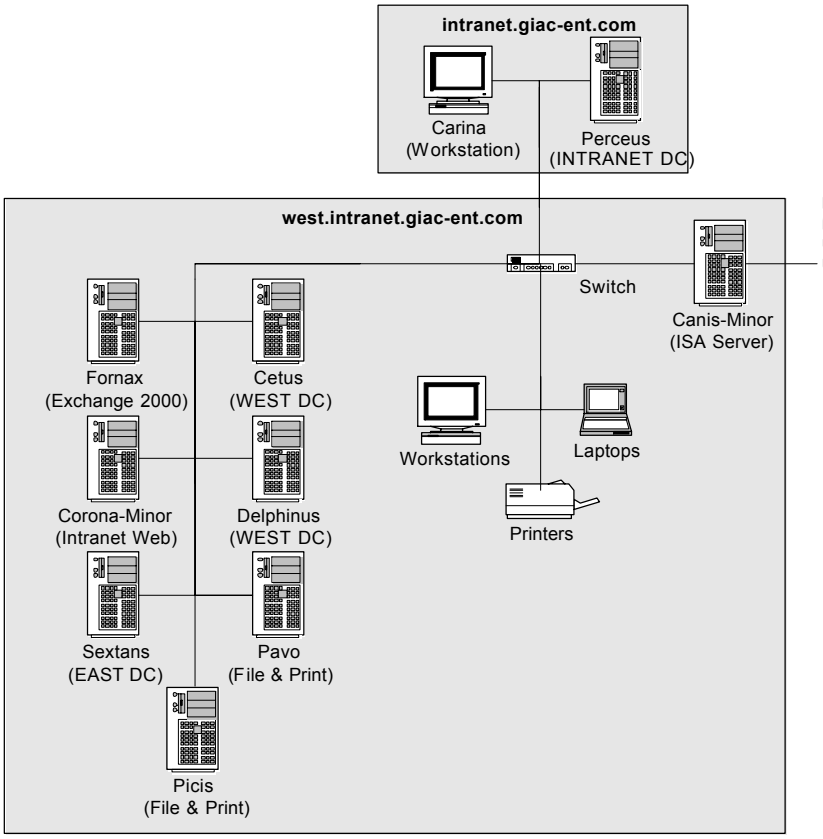

Figure 3, San Francisco Intranet Diagram

Windows 2000 Active Directory Sites

There are two sites in the GIAC Enterprises Active Directory as shown in Figure 4. The Annapolis location has the HQ site, which is on the 192.168.0.0/24 subnet. The San Francisco location has the SF site, which is on the 192.168.1.0/24 subnet. The AD Site structure is shown in figure 4.

A Virtual Private Network (VPN) connection is established between the HQ site and SF site ISA Servers. The intersite communications is routed through the VPN. (See reference 14 for information on how to configure the VPN and routers.) The intersite Active Directory replication is scheduled to occur after work hours at both sites to minimize the impact on the normal work traffic on the ISP connections.

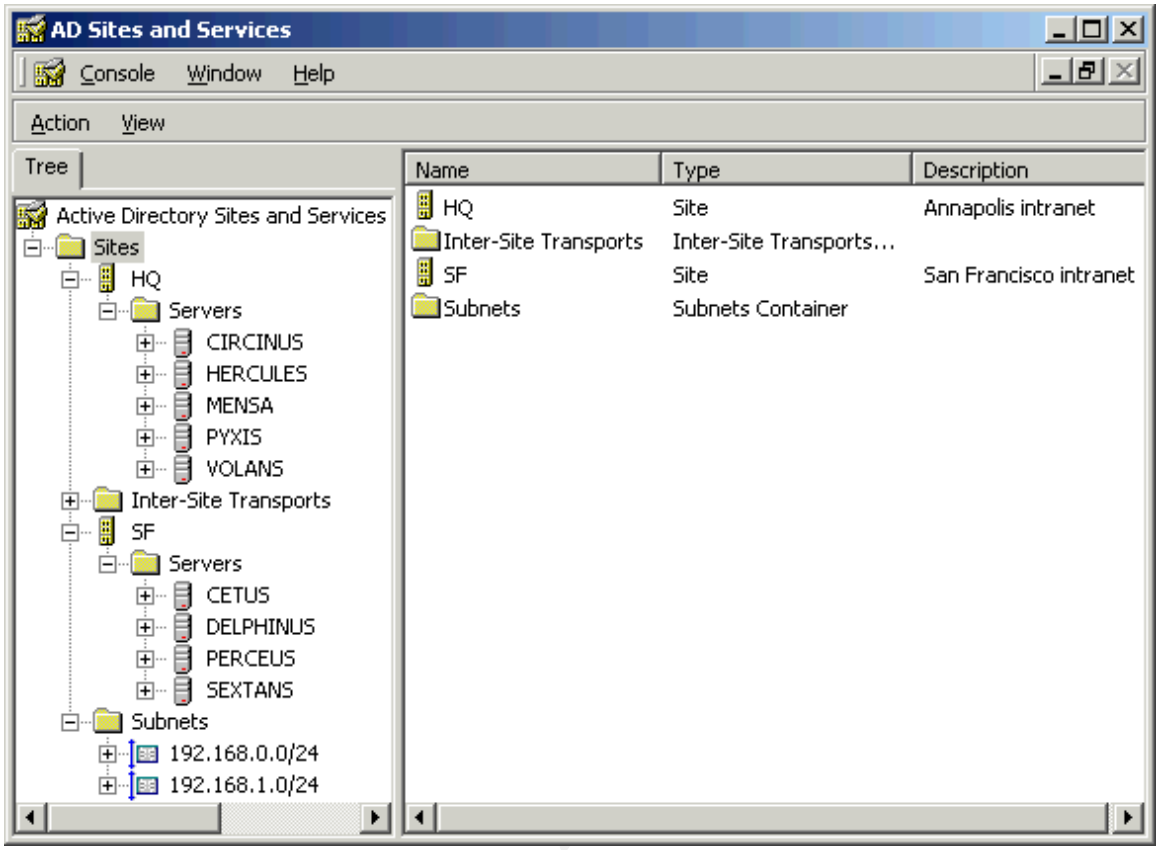

Figure 4, GIAC Enterprises Active Directory Site Structure

Key servers

This section will discuss the major servers in the GIAC Enterprises network. The focus of the discussion will be their role in the network architecture, their location and the reasons for placement in their particular locations. The discussion will also include an overview of the hardware details of each server and the software configuration information. The software configuration includes the operating system (OS) and the application running on that server and will also include information concerning the version and any service packs and hotfixes that have been applied.

Physical Security

All key servers are physically located in secure server rooms that require a correctly coded security badge and a personal identification number (PIN) to be entered into the door locks to enter and exit. Only network and server administrators have the correct badges and PINs. The corporation's physical security contractor logs access to the server rooms automatically. All other personnel are required to sign in to a paper-based log, maintained by the physical security contractor, and be escorted by a network or server administrator at all times.

Other Considerations

- All partitions on the servers are NTFS version 5.
- The POSIX and OS/2 subsystems are removed from all servers including files and registry settings.
- All obsolete directories have been removed from the all servers. The directories are %systemdrive%\DOS, %systemroot%\Cookies, %systemroot%\History, %systemroot%\Temporary Internet Files.
- Set "Do not move files to the Recycle Bin. Remove files immediately on delete." in the properties of the Recycle Bin on all servers.
- Replace the Everybody security group with the Authenticated Users security group on all shares.
- The High Encryption Pack is installed on all computers. The Keymigrt.exe utility is run on each computer, especially important on all DCs, CA, and servers. This utility upgrades the protection of the private keys stored on the computers from 40-bit to 128-bit encryption. This is required following the installation of Service Pack 2 during the Windows 2000 installation. (See Microsoft Security Bulletin MS00-32 and Knowledge Base (KB) article Q260216 for details and to obtain the tool.)
- The SYSKEY.exe utility from the Windows 2000 Server Resource Kit is run on all computers to protect the encryption keys used by the Encrypting File system. For servers, the system key is stored on a floppy that is kept with the server. A copy of the floppy is stored with the backup tapes sent offsite for storage. For workstations the system key is stored on the local system. Laptops have the system key derived from a passphrase that is chosen by the normal user and configured by a Network Administrator.

All servers

- All servers are running Windows 2000 Advanced Server with Service Pack 2. The latest security hotfixes will be applied after they are tested on the test network in the lab. The target for applying the hotfixes is one day after release by Microsoft. Service Packs, both operating system and application are applied after successful completion of lab testing. The goal is to complete the Service Pack deployment within two weeks of the release by Microsoft.
- Emergency Repair disk creation & maintenance schedule. An Emergency Repair Disk (ERD) for is created upon initial installation and configuration of the operating system. Another ERD is created when the application, i.e., Exchange 2000 Server, has been installed and configured and the machine is ready for deployment to the production environment. The ERD is updated prior to installing any Service Pack, hotfix or update to the OS or the application.

Successful installation of the service pack, hotfix, or update is another occasion to update the ERD.

- Back-up schedule including off-site storage and recovery testing schedule. Each server is backed up weekly with incremental backups done daily. Each server machine has an internal tape drive used for the backups. Each server machine has three sets of tapes. Each set has enough tapes to cover the weeks' backup capacity for that machine. Every fourth week a set of backup tapes is sent to the other site for storage and those tapes are replaced in the rotation schedule with new tapes. A test restore to a test server is performed quarterly for each server using a set of tapes that have come back from the offsite storage.
- All servers have the recovery console installed. The permissions on the c:\cmdscon directory and all contents have been set to only Administrators and System have Full Controls and no others.

All computers

- All computers have the creation of 8.3 name generation disabled. This prevents any vulnerability caused by two different files having the same 8.3 name but different long file names and permissions. It is disabled by creating a REG_DWORD value named NtfsDisable8dot3NameCreation in HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem and setting its value to 1.
- All computers have the storage of generation of LAN Manager hashes and storage of them in the Active Directory disabled. This limits the threat of password cracking by preventing the more easily cracked LANMAN hashes from being generated. This sets the value of HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\LSA\NoLMHash to 1 to for "Enabled" and 0 for "Disabled."

Both of the registry changes for all computers have been incorporated in the Workstation Group Policy Object.

Domain Controllers (DCs)

The forest root domain, intranet.giac-ent.com, has three domain controllers. Two DCs are at the HQ site and the remaining one at the SF site. This provides redundancy for the DCs. The DC in the SF site provides the ability to recover the root domain in the case of a disaster at the Headquarters.

Each of the child domains, east.intranet.giac-ent.com and west.intranet.giac-ent.com, has three domain controllers. Two DCs are in the local site and the third in the other site. The DCs are arranged this way to provide the same redundancy and disaster recovery capabilities as provided to the forest root domain. Table 1 lists the locations of the various domain controllers for the three domains

Table 1, Domain Controller Locations

	Site/Location	
Domain	HQ/Annapolis	SF/San Francisco
INTRANET	Mensa Hercules	Perceus
EAST	Circinus Pyxis	Sextans
WEST	Volans	Cetus Delphinus

The domain controllers for the child domains are also DHCP servers in their sites. DHCP servers have approximately half of the site subnet defined in their scopes. The Domain Controllers Group Policy Object (GPO) has additional settings incorporated to secure the DHCP services on the DCs.

Each domain has an Active Directory-integrated DNS zone. All DCs are configured to accept secure dynamic updates from the DHCP clients, i.e., workstations and laptops. Each DNS server has Zone Transfers disabled. All have the "Secure Against Cache Poisoning" setting set.

All unnecessary OS additions, for example Internet Information Server (IIS) and Indexing Service, were not installed or have been removed. The exception is Mensa that is also is the Enterprise Certificate Authority (CA). The CA application requires IIS installed and running on that machine.

Each DC runs on a server class machine that with a minimum of 512 MB of RAM and 20 GB of hardware RAID 5. The DCs for the child domains will be dual Pentium III processor machines to provide the power for all user logins. The root domain DCs are single processor machines with the exception of the DC, Mensa, that also serves as the Enterprise CA which is a dual processor machine.

Each DC will be created with the "Permissions compatible with Windows 2000" option selected. The Directory Services Restore Mode Administrator's password is required by the corporate information security policy to have at least 12 characters and meet the complex password requirements.

Enterprise Certificate Authority Server

Enterprise root certificate authority (CA) is located on Mensa, one of the forest root domain DCs located in the HQ site. The file system security permissions specifically for the CA are shown in Table 2.

Table 2, Enterprise CA File System Security

Object Name	Group	Permission
%SystemRoot%\system32\certsrv	Administrators Authenticated Users SYSTEM	Full Control Read and Execute, List Folder, Read Full Control

%SystemRoot%\system32\CertLog	Administrators CA Administrators SYSTEM	Full Control Full Control Full Control

The Enterprise CA was installed with the optional High Encryption Pack installed. The Enterprise CA key pair is 4096 bits long and was generated using the Microsoft Enhanced Cryptographic Provider v1.0 set as the cryptographic service provider (CSP) and SHA-1 as the hash algorithm. The enterprise root CA will be backed up manually using the Certificate Authority MMC snap-in.

Users are required to request certificates from the enterprise CA using the Web Enrollment support pages that have been secured using SSL and a certificate generated by an external CA (Verisign). The Workstation OU Group Policy Object configures computer to automatically request certificates. To limit the types of certificates to be issued by the CA, all unnecessary certificates templates are removed from the Policies container of the enterprise root CA in the Certificate Authority snap-in as shown in Figure 5. If there is a need to create a certificate from a template that is removed, it can be added back into the Policy Setting container long enough to issue the certificate.

Figure 5, Enterprise CA Policy settings

The security setting of all certificate templates have adjusted, via the Certificate Templates container, shown in Figure 6, in the Public Key Services folder under the Services Node of the Active Directory Sites and Services MMC snap-in, to remove normal users from accessing them, with the exception of the User template. The User Template is set to allow Authenticated User to enroll.