Global Information Assurance Certification Paper

John H. Campbell

Securing Windows GCNT Practical Assignment
Version 3.0 (revised August 13, 2001)
Option 1-Design a Secure Windows 2000 Infrastructure

The Cookie *DOESN'T* Crumble

Network Design Plan for GIAC Enterprises, Inc.

Table of Contents

Chapter 1

About GIAC Enterprises

Assumptions and Relevant Details

The Company

GIAC Enterprises is neither truly a start-up nor a Fortune 500. The founders have been in business for about 15 years, serving the restaurant trade with custom software and fortune cookie printing solutions. They decided to ride the Internet wave about five years ago, and this part of the business has become the primary activity. Overall employment is about 100.

Locations of Operations

GIAC Enterprises operates a total of three sites, including a provider site where its production e-business servers are co-located.

The primary site is located on two floors of a suburban office building in the Gateway Park Business Center. This location is usually referred to by company insiders as 'Park 10', after the number on the building. Most of the firm's operations are located here, including Executive, Finance, Human Resources, Information Technology, Sales & Marketing, and Customer Support.

The Research & Development Department formerly operated out of two rooms of the Chief Technology Officer's house, but owing to staff growth and pressure from the Board of Directors, the CTO recently relocated it down the street to the upper floor of an historic building in downtown Hicksville (the outlying burg he calls home) around the corner from his favorite pizza joint.

The production infrastructure lives at a co-location facility, run by an internet hosting company that's been bought out twice in the last two years. Fortunately, service levels have remained relatively bearable throughout. The co-lo facility itself is a non-descript, windowless concrete box in an industrial park near the freeway. It was formerly occupied by an industrial supply company, and the associated signage has been left in place in an attempt at 'security by obscurity.'

Current Departmental Technology Environment

GIAC has been around long enough to accumulate a variety of technologies. This is the main reason they're looking at rolling out a comprehensive Windows 2000 infrastructure. Moreover, the firm has a bit of a split personality – it's partly a cutting edge internet company, and partly a stable and somewhat stodgy established firm.

At the main site, most employees in most departments are using a variety of Intel clients running Windows 98 or 2000, with a few exceptions. The graphic artists who produce marketing collateral and the company newsletter are Mac people, and some of the IT guys are Linux fans. Everyone will migrate to Windows 2000 Professional, including the Macheads, but they'll get to keep their Macs as well (compromise is the mother of getting things done.) Those Intel clients running at 500 MHz or better, capable of an upgrade to 256 MB of RAM, and possessing big enough hard drives (say, 10 gigs or better) will stay. Yes, I realize those are tougher standards than Microsoft's published recommendations. These keeper machines may be migrated to less demanding users. The rest of the clients will be out the door, replaced by new Pentium 4 or Athlon machinery. Internal IT is working on identifying the hardware and putting the PO together.

A Linux box of uncertain vintage and rev level runs the existing corporate website. It was established as a joint project between a junior R&D staffer and Sales & Marketing. A newly hired webmaster has been readying a new site, and it will be hosted on an IIS 5.0 server.

There's an NT server in place, running Exchange 5.5 to support internal email and calendaring. It will get migrated to Exchange 2000 on Windows 2000 at some point. There's also an existing Windows 2000 server, providing file and print services to most users. These two machines are the DCs for an existing NT domain.

Executive, Finance and Human Resources access a Novell 4.x server, which hosts a copy of GIAC's old restaurant industry accounting package. They are hiring a CPA firm to migrate them to the latest and greatest third party ERP package, once the new infrastructure is in place. They want their own server, for perceived security and to make it easier for their migration project. Their existing client PCs are already set up for NetWare connectivity and running DOS apps (like the GIAC accounting program) so they will stay in place until the new ERP package is in production.

Sales and Marketing doesn't have any unique technology needs beyond the Macs and their associated publishing industry-oriented peripherals. They do have a huge PowerPoint and press dump on the Windows 2000 server. They keep their contact information on the Exchange server and access it via Outlook clients. The Macs also have a share on the Windows 2000 server.

Customer Service keeps their help desk database on an old Solaris box that served as GIAC's very first production internet server. It's getting long in the tooth, and the help desk vendor has had a Windows solution on the market long enough for it to be stable and feature equivalent to the Unix edition. IT has been testing this product, and is preparing to

roll it out to production as part of the new Windows 2000 environment. Customer service is looking forward to ditching the old X-Window based incarnation of this package. So is IT.

R&D has two networks. One is connected to the Internet, and is used for email, web access, and general productivity. The clients are a mixture of Linux and Windows NT/2000 machines, depending on the preferences of the individual engineers. The R&D site also has a standalone lab network, which is not connected to the Internet in any way. This latter network is a clone of the co-located production environment, albeit using last year's servers.

The production infrastructure is Unix-based, with heavy reliance on custom software, backend relational databases, and third-party certificate management and credit card transaction processing. We aren't privy to any of this, and it doesn't affect this project anyway-phew!

Client Expectations & Scope of Work

GIAC wants us to migrate its network to a Windows 2000 Active Directory (AD) based environment, as follows:

Install a new server as the FSMO master for the new corp.giac.net domain. Secure it appropriately.

Bring the existing Windows 2000 server into the domain and secure it. It will serve as a file/print server and a domain controller.

Install a new server for the company ERP package and secure it. It will contain payroll, HR, and other sensitive information.

Bring the new helpdesk server into the domain and secure it.

Make sure the NT 4/Exchange 5.5 server functions in the new environment. It will be upgraded or replaced later.

Install a new server to host the www.giac.net corporate website. Secure it properly. Content will be responsibility of the webmaster.

Build a new server for R&D. It will be a domain controller, file and print server.

Set up Active Directory and appropriate Organizational Units, Groups, and Group Policy to support the users and new network client computers.

Review the security of the network itself and make appropriate recommendations.

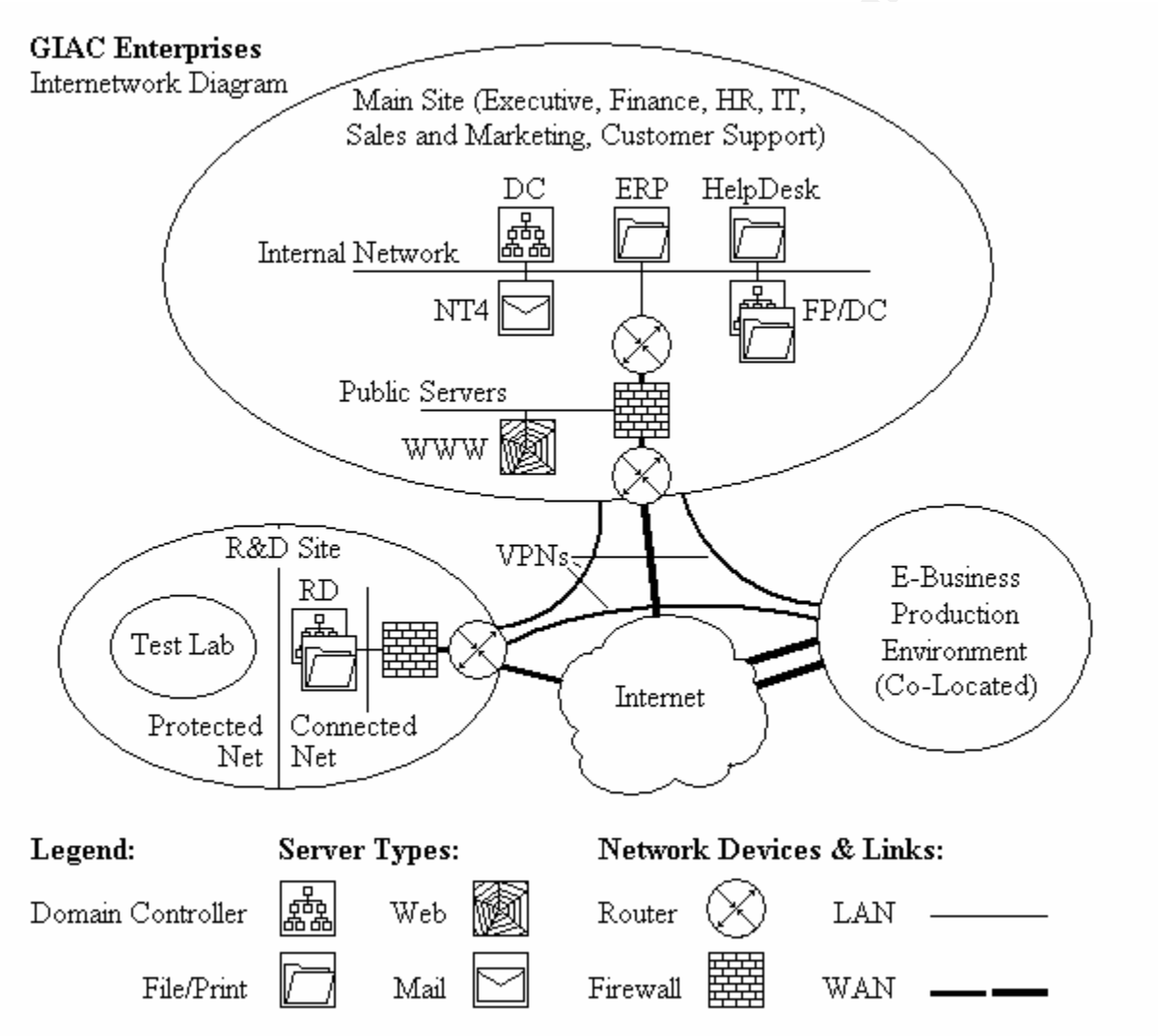
Be sensitive to the fact that GIAC uses and values technologies other than Microsoft's. Deploy MS where it makes sense; use other products when they make sense.

Document everything to the level IT needs to understand, maintain, and develop the network.

Chapter 2

Proposed GIAC Physical Network

Description of Sites, Servers, Infrastructure



- Figure 2.1: GIAC Enterprises Proposed Internetwork Diagram

Main Site

Park 10 (the main site) is connected to the Internet via several T-1s connected to an inverse multiplexer. A Cisco PiX firewall protects the perimeter. It sits behind the provider's router, and another router sits behind it to allow a multinetted internal IP environment. A switch fabric provides connectivity for servers, workstations, printers and other devices on the LAN. Alternatively, internal routing and switching could be combined by using a Layer 3 switch.

We want to secure most of the traffic amongst the three GIAC sites – Park 10, R&D, and the Co-lo facility. Owing to the availability of the PiX, we will look at upgrading it with a cryptographic co-processor board and using it to terminate LAN-to-LAN VPNs with the other two sites. If this doesn't scale well enough to handle the traffic, we'll look at a dedicated VPN device. We could do an MS VPN solution, but since the PiX is already there, I can skip the research and testing that would be needed to size the MS solution. The Co-lo facility will handle the setup at their end. We'll look at R&D's needs shortly. For a good start to reading up on PiX VPN solutions and configurations, see

http://www.cisco.com/warp/public/471/top_issues/vpn/pixvpn_index.shtml.

The new IIS 5 web server will live on one of the PiX's DMZ ports. We'll set the PiX up to let TCP ports 80 (HTTP) and 443 (HTTPS) through from outside. Access from inside should be no problem, as PiXes default to allowing traffic from higher-security segments (inside) to lower security segments (DMZs and outside.)

The web server will be set up with separate partitions for the operating system and the website itself. It will have dual processors and lots of RAM (let's say a gig since memory is so cheap these days.) The system partition will be a mirrored pair of hot-swappable SCSI disks. The website partition will be either a mirrored pair or a RAID5 array (hot-swappable either way) depending on the amount of data that must be kept. I favor using hot-swap drives, mirrored pairs and RAID 5 arrays because hard disks are cheap but downtime isn't. All the servers will be set up this way. Using two partitions may improve performance, depending on the application. It also helps protect the server from directory traversal attacks and other attempts to access privileged commands and resources. We'll put a DLT tape drive on board and use either NTBackup or ARCserve (http://www.ca.com/arcserve) for backups.

The web server will be carefully hardened. It will not be part of the Windows 2000 domain. SP-2 and appropriate hotfixes will be installed. Every partition will be NTFS v.5. Unnecessary services will be shut down. Unnecessary software interfaces will be disabled. Administrative command executables will be corralled and protected with DACLs. We'll unbind NetBIOS from the network interface. We'll equip the box with anti-virus software to catch any attempts at placing Remote Access Trojans (RATs) on it. We'll also make sure the IUSR account has no privileges other than read/execute in any of the web content directories, and no privileges whatsoever anywhere else on the system. Same goes for the group "Everyone" – just the minimum needed. This is not an exhaustive list of hardening steps. SANS' "Securing Internet Information Server 5.0" curriculum will be consulted.

Another good source of info is the installation and configuration checklists in "Securing Windows NT/2000 Servers for the Internet" by Stefan Norberg.[1]

The mail server ('NT4') will be left alone for the time being. Internal IT is going to build a new Exchange 2000 server once the dust settles from this project. The current machine is a BDC for the NT environment. It will end up as the PDC. We will set up a trust between it and the new AD domain. We'll stay in mixed mode until Exchange is upgraded and all the clients are migrated. The new mail server won't be a Domain Controller. NT4 has an 8MM tape drive and uses NTBackup.

The new Domain Controller (DC) will be a rack mounted, twin processor server with a gigabyte of ram and four hot-swappable SCSI drives. The drives will be set up as two mirrored pairs. The first pair will hold the OS and the AD Log; the other will hold the AD database. This is overkill to a certain extent, but it gives us maximum redundancy for the machine that will be our FSMO master and our first domain controller. It won't run any file shares. This machine, along with the other DC and the two application servers, will run ARCserve agents and be backed up across the network to a tape library.

The remaining three file servers at the main site are rack mount, beefy machines. They have or will have, two processors and a gig of RAM. They will have mirrored system volumes and RAID5 arrays for data.

The "FPDC" server will have the main file shares and network print shares. (Most of the printers at Park 10 are network attached.) This machine will serve as a Domain Controller. It will also serve as the ARCserve host for backing up itself and other servers. This is the current Windows 2000 server. Owing to the creation of the new domain and the installation of Active Directory, we're going to bite the bullet and wipe this guy after taking and verifying a couple of backups. This will ensure that no NT issues of any sort remain on the box, which makes me feel more comfortable than merely importing and applying the 'basicdc' Security Template with Group Policy.

The Executive, Finance and HR groups will be served by a separate server we'll call ERP. It will have file shares for these groups, and will also support the new ERP package the CPA firm has been hired to install. It will run an ARCserve Agent.

The Customer Service group will be served by a separate server we'll call HelpDesk. It will host Customer Service's online documentation and the new Help Desk software package. It will run an ARCserve agent.

R&D Office

The R&D Site has a single T-1 at the present time. It also has a SoHo – type firewall product that will be yanked and replaced with a PiX so we can do VPNs to Park 10 and the Co-lo site more easily and with greater capacity.

We're going to install a new Windows 2000 server (called "RD") that will serve as a DC, file and print server. The DC will give R&D some redundancy in case network problems cut

them off from Park 10, and will also improve authentication and DNS lookup performance. We'll use a tower because they don't have a formal computer room with racking installed. Other than that the specs will be similar to the servers at Park 10 – two processors, 1 gig of RAM, a mirrored pair of SCSI drives for the system volume, and a RAID5 array for the file shares. All the drives will be hot-swappable. We'll do a DLT drive here and run the backups locally with NTBackup. This will save us from killing our T-1 with ARCserve. We'll have to make sure the backup tapes get cycled out to offsite storage, but the daily courier from Park 10 can handle that. Backup logs will be reviewed remotely by IT staff at Park 10. Since AD DCs aren't read-only like NT4 BDCs are, we'll have to lock up RD. That means the R&D staff will have to do some housecleaning and clear out one of their storage rooms – horrors!

Windows 2000 Service Packs and Hotfixes

All the Windows 2000 servers will be installed with Service Pack 2 and a selection of hotfixes (software patches that fix specific problems.) Hotfixes currently available for each Microsoft product can be obtained from Microsoft's TechNet website at the following address:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp

This page presents a form titled 'Search by Product and Service Pack.' Choose the product from the Product pick list, then the Service Pack level from the Service Pack pick list, then click the Go button. The hotfixes available for the product that are appropriate for the SP level will then be displayed as links you can follow to read the associated Security Bulletins.

According to Harry Brelsford,

> Hotfixes are not regression tested. This means that the fix has not been fully tested in all scenarios in a production environment. For this reason, it's recommended that you apply hotfixes only for specific problems that you may be experiencing. Some hotfixes are more important than others or may upgrade a specific component that isn't on the system to be upgraded. You should apply a hotfix only after reading the descriptions of the problem and of the hotfix solution itself in the Microsoft Knowledge Base article that accompanies the hotfix.[2]

Based on this advice, we'll read the Security Bulletins for each of the hotfixes we find on Microsoft's list and apply only the ones we need. I tend to skip the ones that update functionality I don't use (like NetMeeting and HyperTerm) or that repair minor Denial of Service vulnerabilities (in the case of internal servers.)

Service Packs and Hotfixes can be pushed out to computers by Group Policy. In the case of building the new machines for this rollout, I'll do it manually. I'll begin by loading Windows 2000 with SP-2 slipstreamed into it. John Savill's Windows NT/2000 FAQ website tells how to make a bootable Win 2000 CD updated with SP-2. Here's the link:

http://www.windows2000faq.com/Articles/Index.cfm?ArticleID=21331&Key=Windows%202000%20Service%20Pack%202%20%28SP2%29[3]

Once the install is complete, I'll load my chosen hotfixes as a batch using qchain.exe (see Microsoft Knowledge Base Article #Q296861 for details on using qchain.)

Other Services and Issues

Many of the following topics could easily be placed under the heading 'security issues that can't be resolved with Group Policy.' But some of them also bear on the layout and function of the network itself. Therefore, we'll include them with the purely network infrastructure oriented items and discuss them all now.

We'll use DHCP to distribute IP addresses and other IP config details such as default gateways and DNS. We'll use a split scope at Park 10 – each of the two DCs will have a pool of IP addresses to give out, so that we have some redundancy. The server at R&D will host the scope for that site. Hosting DHCP services on Domain Controllers isn't generally considered a good idea, but it's a trade off we can live with for a couple of reasons. First, all the DHCP clients on the network will be Windows 2000 machines, so they can update their own DNS records – they don't need the DHCP server to do it for them. Therefore, we don't have to put the DHCP servers in the DNSUpdateProxy group. Second, we're lacking available servers to put DHCP on. We don't want to burden departmental application servers or the mail server with hosting DHCP services, and there aren't any servers at R&D besides the DC – if we don't put DHCP on RD, there will be no local source of DHCP leases at all, and that's unacceptable from a network reliability standpoint. Clients couldn't even attach to the network without a valid IP address.

We'll have our internet provider handle DNS for the outside world. This should be limited to just the production site, our corporate web server and mail server. This will serve to protect internal servers from DNS-based attacks and hacker reconnaissance coming from the Internet. Active Directory-integrated DNS will run on each DC to serve the internal network, forwarding queries they can't resolve to the provider's name servers. We'll harden internal DNS by enabling Secure Dynamic Updates (DNS snap-in, Domain Properties, General tab) and Secure Cache Against Pollution (DNS snap-in, Server Properties, Advanced tab) just in case some internal wannabe decides to do a bit of playing around.

Antivirus protection will be provided through Trend Micro products (http://www.antivirus.com.) (This is not an endorsement per se, it just what I'm familiar with. The main issue is to have centrally managed, self-updating AV protection in as many places as possible.) We'll run ServerProtect (realtime and scheduled scan) on each server, ScanMail for Exchange on the mail server, and OfficeScan (realtime and scheduled scan) on each client. All of these products report to a central console, and all machines acquire updates for scan engines and signature files from a central share, which is updated by a service that downloads from Trend periodically.

For remote access, GIAC can go one of two ways: use RRAS on one of the servers for dialup and / or VPN access, or equip people with Cisco VPN client software. This is too big a topic to deal with seriously here. SANS Securing Windows 5.3 curriculum discusses RRAS security.

For remote administration, we'll put Terminal Services on every server. Set up in Remote Administration mode, it's a great way to avoid trips to the computer room. Terminal Services can be selected for installation while installing the Windows OS, or added later through Add/Remove Windows Components under Add/Remove Software on the Control Panel. To access a Terminal Services machine remotely, you need client software. Client software images can be found on any TS-equipped machine under %systemroot%\system32\clients. Remote administration rocks for clients, too, but we'll have to use a third party product like VNC for that (http://www.uk.research.att.com/vnc) as Windows 2000 Professional doesn't support Term Services.

To assist in data protection on clients, we'll redirect My Documents and certain other folders to a big network share. For laptops, we'll configure Offline Folders so their users will still have access to their files when on the road. We will also look at Encrypting File System for laptops to protect important corporate data in the event of theft or loss. SANS Securing Windows 5.2 curriculum covers EFS, with or without a PKI infrastructure installed. We'll talk more about Folder Redirection in Chapter 4.

Firewalls need to be set up under an Inbound Implicit Deny All policy. This states that no traffic will be allowed into the internal network from outside unless it is expressly permitted. This is the only way to go nowadays, because so many services are running on our nets and so many cracking tools (especially Remote Access Trojans like SubSeven and BackOrifice) can be configured to run on any port. We need to treat our nets as our property, to be shared only as we see fit. On the outbound side, we can use an Implicit Allow All policy, closing down only those things that are expressly against organizational wishes. Obviously, the firewall used has to be smart enough to manage session state so that traffic coming in on an arbitrary port in response to a request from an internal client, will be allowed through.

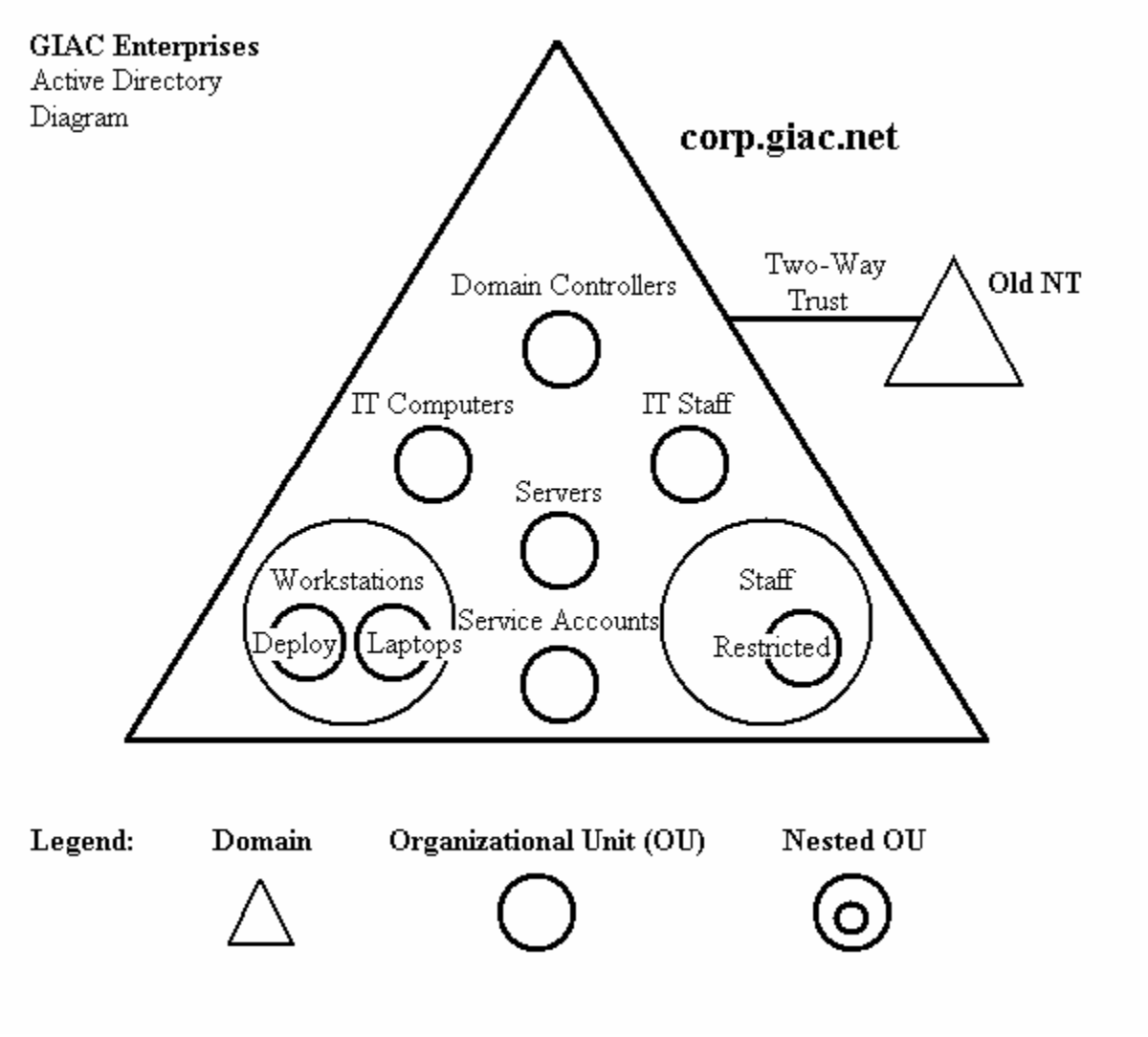
SNMP (Simple Network Management Protocol) is prevalent on nearly every piece of networkable gear these days-switches, routers, printers, Windows 2000. Even though we'll block outside access to snmp with the firewalls, it's still not a very secure protocol. Either we assign nasty community strings (which are the equivalent of passwords and are transmitted in the clear) or manage by other means and turn snmp off. The latter is preferred, in my opinion, except when you need the functionality (for switch or router management) and other means are not available. In this case, see if you can configure the device to accept management only from certain IP addresses, and to send its traps only to those IPs.

Last but not least, I'd like to see a mail relay set up on a dmz to conduct mail in and out of the internal network. This would protect the internal mail server, which is part of the domain, from exposure to the Internet. The relay might be something as simple as a hardened Linux box equipped with the latest edition of sendmail, or we could use Microsoft's Internet Security and Acceleration Server (ISA.) An added benefit of using ISA Server would be the ability to publish, or 'reverse proxy' our corporate website, further protecting it from crackers. Websites helpful for learning about this product include http://www.microsoft.com/ISAServer and http://www.isaserver.org.

Chapter 3

Proposed GIAC Active Directory Layout

Rationale for Domains, Sites, OUs, Security Groups



- Figure 3.1: GIAC Enterprises Proposed Active Directory Diagram

Active Directory is capable of supporting a very elaborate and confusing organizational structure. To make things easy to understand and administer, we'll try to apply simplicity wherever possible. A simple design is inherently more self-documenting and less prone to administrative error. Therefore we are less likely to introduce security holes due to overlapping, conflicting Group Policy settings.

Domains

GIAC Enterprises is a fairly small company. It doesn't have divisions or subsidiaries. It operates at three locations, and has a single, centrally-managed IT function. There are no divisional administration issues, and no need to restrict replication. It is not economically justifiable to install extra domain controllers to support an empty root domain. For all these reasons, and to maintain simplicity, we'll go with a single domain architecture.

Since the giac.net domain is already live on the Internet, the new domain will be known as corp.giac.net. This zone will be hosted on Active Directory-integrated DNS running on the domain controllers. Using a DNS subdomain for our corporate zone will make any future DNS integration easier, and AD integration allows us to turn off zone transfers, improving security.

The Windows 2000 Server Resource Kit Deployment Planning Guide tells us what to do about Global Catalog Servers:

> In a single domain environment, global catalog servers are not required to process a user log on request. However, you should still designate global catalog servers … Clients still seek global catalog servers for search operations. Also, having global catalog servers already in place allows the system to adapt gracefully if you add more domains later.[4]

So, we'll make all the servers except our FSMO master into Global Catalog servers. The FSMO master is off the hook because an Infrastructure Master shouldn't also be a GC server. See KB #Q197132 for details.

Trusts

We'll be supporting the old GIAC NT domain for awhile until all the users migrate and the old Exchange server is retired. This server, 'NT4', has been a BDC. It will be promoted to PDC (the old PDC will be wiped and become 'FPDC' – a file/print server and domain controller.) An explicit two-way trust will be created between corp.giac.net and Old NT. Given that we're a single domain, 'shortcut trusts' are moot.

Sites

We will create two sites, Park10 and RDOffice. The domain controllers DC and FPDC will live at Park10, along with several member servers. The controller RD will live at RDOffice. There will be one site link, called Park10-RDOffice. All three DCs will be Bridgehead servers (for simplicity and redundancy.) Replication defaults will be left in place for servers

at Park10, owing to prodigious available switched network bandwidth. However, the R&D office has only a T-1 to reach the world with, so we'll set up replication with Park10 to happen between midnight and 5:00 AM, daily. If this proves too limiting, we can open it up over the noon hour, at the risk of annoying network gamers at the R&D site.

Organizational Units (OUs)

GIAC uses a centralized IT function so no delegation of control is needed. We're not going to buy into the notion of building a complicated hierarchy of OUs to match our business structure- especially not for a firm of 100 employees. Instead, we'll set up OUs strictly for ease of administering and applying Group Policy.

For ease of understanding if not ultimate simplicity, I'm going to set up separate batches of OUs for user accounts and computer accounts. Then we'll disable the User portion of the GPOs that apply to computers, and the Computer portion of the GPOs we apply to users. Keeping OU nesting to a minimum will keep GPO processing humming. It might be nice to use the generic domain containers for computers and users provided in the domain, but according to Will Willis, et al, "GPOs *cannot* (emphasis theirs) be linked to the generic AD containers." [5] Indeed, they cannot, so we'll assign a few domain-wide things in the Default Domain Policy, and save the rest for lower level OUs.

One thing in particular we're trying to accomplish with this OU structure, is to avoid any need for messing with inheritance and overrides- it's much easier to understand and manage policy when there isn't any of *that* going on behind the curtain.

Computer OUs

We'll start off by utilizing the built-in Domain Controllers Organizational Unit. DCs are few in number and require specialized GPOs.

Next, we'll consider the rest of the computers.

Member Servers are our next category of machine – their needs are similar in some ways to those of DCs, but they may be hosting application programs as well. So we'll set up a Servers OU to put them in.

IT Computers will be placed in their own OU. IT staff machines typically have very unique requirements – they must be more secure in some ways but less locked down. Their users typically are knowledgeable and need flexibility more than standardization. They may run unique software not present elsewhere in the organization, and they may perform management functions that require service accounts or greater access to the local machine. Generic Workstation GPO would serve them poorly. Although there are other ways of handling the differences and conflicts between ordinary workstations and IT ones, I like the self-documenting simplicity of collecting IT computers in their own separate OU.

Staff workstations will all be configured in a similar manner, so we'll create one Workstations OU to put them in. Laptops will require slightly different configuration (I'm thinking especially

of setting up Offline Folders so the users will be able to get to files when disconnected from the corporate net.) We'll create a nested OU called Laptops within the Workstations OU. That way laptops will receive all the standard GPO stuff for Workstations, plus any special policy they need.

The other nested OU in Workstations is called 'Deploy.' When we have a big software deployment, we'll run batches of workstations through this to avoid the demand on bandwidth and server shares that would be caused by every computer in the place requesting the software simultaneously.

User OUs

Most users can benefit from a standard set of GPOs, so we'll set up a Staff OU as a place to deploy standardized Policy for users.

Within the Staff OU I have created a 'Restricted' OU, as a place where we can quarantine anybody who needs additional policy (and we all know who those folks are, don't we?)

Many services and programs require service accounts, and those accounts need special treatment (for one thing, their passwords can't expire.) They get their own OU called Service Accounts.

Lastly, IT workers get their own OU called IT Staff, so that we can tune their policy to meet their unique needs. This will largely consist of exempting them from the restrictions we give everyone else!

Security Groups

The Deployment Planning Guide makes the suggestion: "Because resource access is granted using security groups, you might find that your business organizational structure is best represented in security group structures instead of OUs."[6] We will make use of this concept to help limit access to resources such as network-based applications and file shares.

Recall that GIAC is administratively divided into several departments: Executive, Finance, Human Resources, Information Technology, Sales & Marketing, Customer Support, and Research & Development. We will create Global Security Groups for each of these departments, as well as whatever other groups are needed for convenient administration. Once we get to Exchange 2000 and Native Mode, we'll also create a Global Security Group with everyone in it, and use that for company-wide emails and to control access to network printers. (So far it hasn't proven necessary to limit printer usage by group. Other companies might want to create special groups for special printers, or to dedicate printers to particular departments.)

Next, we'll create Domain Local Groups for several resources we want to provide restricted access to, and add the appropriate departmental Global Groups to them:

- The ERP server – only Executive, Finance and HR people need to access the application and file shares on this guy, so those groups will be given membership in the local groups for these resources.
- The HelpDesk server – only Sales & Marketing and Customer Support need access to this resource.
- The RD server – the R&D group needs access to its file shares.
- The FPDC server – various departments keep shares here, including Sales & Marketing (Macintosh and PowerPoint/press dump shares.)

Chapter 4

Proposed GIAC Group Policy Setup

Settings and Rationale

Anatomy of a Group Policy Object (GPO)

The easiest way to get to GPOs on your system is to open the Active Directory Users and Computers snap-in, right click on a domain or OU, and click on the Group Policy tab. This will reveal all Group Policy Objects linked to the domain or OU. If you then select a GPO and click the Edit button, an MMC-style expandable outline will appear in the left portion of the Group Policy snap-in, with room for details on the right.

GPOs are divided into two sections or nodes, Computer Configuration and User Configuration. Even though both entity types can be dealt with in the same GPO, we won't do it that way. We'll build Computer Configurations for computer OUs, and User Configurations for user OUs. Then we'll disable the unused portion when we link the GPO to an OU.

Software Settings

Both nodes have child nodes called 'Software Settings.' This is "a location for independent software vendors (ISVs) to add further extensions. If no nodes have been added by ISVs, then Software Settings contains just the Software Installation extension included with Windows 2000."[7] This bit of info comes from the Windows Resource Kit, Distributed Systems Guide, which is very helpful in understanding the intricacies of Group Policy.

Windows Settings

Both nodes also have child nodes called 'Windows Settings.' The contents of these vary quite a bit between Computer and User nodes, so we'll look at them separately.

For the Computer Configuration node, Scripts and Security Settings are available. The Scripts child node allows you to assign scripts that will run on machine startup or shutdown. The Security Settings child node has a bunch of stuff that collectively covers a lot of what we want to do in Group Policy. Here's a list, adapted and condensed from the Distributed Systems Guide:[8]

- Account Policy controls things like password length, account lockout details, and Kerberos settings. These items can only be set at the Domain level.
- Local Policies affect the local machine's auditing, granting of user rights, and various security-oriented settings.
- Event Log controls how Event Logs get controlled and managed.
- Restricted Groups can be used to limit Group memberships.
- System Services controls how services start and who can mess with them.
- Registry controls security for Registry keys.
- File System handles NTFS Permissions.
- Public Key Policies is for everything to do with PKI – certificates, trusts, EFS Recovery Agents, etc.
- IP Security Policies – whether and how clients and servers communicate securely using IPSec protocol.

On the User node, Windows Settings includes Internet Explorer Maintenance, Scripts, Security Settings, Remote Installation Services, and Folder Redirection.

Internet Explorer Maintenance does what it says, and scripts can be used to assign scripts or batch files that will run when a user logs in or out. Security Settings is much more brief than it is on the Computer node. It only has one child node – Enterprise Trust, which is used for configuring Certificate Trust Lists for users. Remote Installation Services is used for configuring the automated installation of the Windows 2000 OS on a client computer. This is a big topic in itself, one we won't be considering here.

Folder Redirection allows you to put the user's Application Data, Desktop, My Documents and Start Menu folders someplace besides a subdirectory under Documents and Settings on the client hard disk. We're going to use this feature to store people's documents on a server home directory share, so that their data will get backed up.

Administrative Templates

This is the final child node under both Computer and User nodes, although the contents vary between the two. Administrative templates give you all the power you used to get (and then some) with NT System Policy and TweakUI. Everything in this section basically does one thing – sets Registry values to control or limit system and application functionality. Unlike NT System Policy, which applied registry tweaks essentially forever (until they were explicitly changed), Group Policy manages settings actively, rolling them back when a given GPO is no longer applied. The end result is much more control and less hassle for the administrator.

Owing to the quantity of settings available under Administrative Templates, I'm not going to run through them here. We'll look at the appropriate settings when we go through the specific GPOs.

Importing Security Templates

Microsoft provides several Security Templates that can be merged into Group Policy Objects. These serve to provide a baseline configuration when you're setting up a new GPO. New ones can be created, and the existing ones can be edited.

Templates can be accessed from the Group Policy snap-in while you're editing a GPO for a given domain, site or OU. Open up the Computer Configuration node, then Windows Settings. Right click on Security Settings, then choose Import Policy.

There are quite a few templates available, but they're all classified by name into Basic, Compatible, Secure, and High Secure, and for use on workstation, server or Domain Controller computers.

Basic templates are equivalent to the settings put in place when you do a clean install of Windows 2000. They are intended to be used to clean up settings on machines that have been upgraded from Windows NT. Hopefully we won't be doing any of that.

Compatible templates are designed to dumb down the standard settings so that older applications can run. As the Distributed Systems Guide says, "This is not considered a secure environment."[9] We won't touch these with a ten foot pole!

The Secure templates provide enhanced security over the Basic ones and will be our default for import into the GPOs we create.

Some interesting things are said about the High Secure templates. The W2K Directory Services Exam Cram describes them thusly:

> Goes beyond the secure template to extreme security measures. In doing so, it has no regard for functionality, performance, connectivity with non-Windows 2000 clients, or ease of use."[10]

Sounds like fun when you're trying to get a network up.

Furthermore, Phillip G. Schein, writing in the W2K Security Design Exam Cram, advises that the High Security templates "are for IPSec-enabled network traffic and protocols…All network communication must be digitally signed and encrypted."[11] This sounds to me like overkill for the GIAC environment, at least for now.

Domain-Level Policy

Account Policy settings can only be applied at the Domain level. Therefore, that's where we'll do them. But we won't do anything else at the domain level. That's what the OUs are for. There are a few other things that might apply to everybody (having 'logoff' appear on

the Start Menu, a standard DNS suffix, or warning everyone to change passwords 14 days in advance of their expiration.) But I could see admins forgetting where they set that stuff up two years ago, so for simplicity and ease of documentation, we'll just leave it at Domain Account Policies only. We'll disable the User Configuration part of the domain GPO to speed its processing up, and we'll remove all the Administrative Templates, since none of their settings are relevant here.

To choose appropriate settings, we'll review the Computer Configuration>Windows Settings>Security Settings>Account Policies settings that are in the Secure Workstation Security Template. We won't actually import that template, because it configures other stuff we don't need at the domain level. We'll be a bit more relaxed on a couple of the password policy settings than securews.inf is, to avoid widespread hate and discontent among the users. We're also more relaxed in some respects than the SANS curriculum recommends for the same reasons (Securing Windows 5.1, p 68.) This is what we'll set up:

Password Policy:

- Enforce password history: 24 remembered (from template; SANS curriculum suggests 8 to 13.)
- Maximum password age: 42 days (from template; SANS says 45 to 90.)
- Minimum password age: 2 days (from template; SANS says 5 days-keeps users from just changing them through a batch of 25 to get back to the one they like.)
- Minimum password length: 8 characters (template; SANS says 8-14.)
- Complexity requirements: Disabled until IT does a class or a memo on how to come up with successful passwords (securews.inf and SANS have this Enabled.) A better solution to strong passwords would be smart cards, IMHO.
- Reversible Encryption: Disabled.

Account Lockout Policy:

- Account lockout duration: 4 hours (SANS; template says 30 minutes. That will save you from scripted attacks even on long weekends.)
- Account lockout threshold: 5 invalid logon attempts (both.)
- Reset lockout timer: 30 minutes (template; SANS wants 15.)

Kerberos Policy: neither the Secure Workstation template nor SANS Best Practices mess with these. We won't either.

GPOs for Computer-Oriented OUs

Domain Controller Group Policy will start with importing the Secure Domain Controller Security Template. We'll undefine all the Account Policy stuff we set up on the domain itself, and delete the Administrative Templates that just make the GPO file bigger.

Next, we'll go through the Local Policies settings and compare them to the 'Best Practices for Account Settings' section found in SANS Securing Windows 5.1 curriculum, page 68. In general, the Secure DC Template is fussier than the Best Practices list. Here are a few of the differences:

- The Secure DC template audits more things than Best Practices calls for – we'll follow the template.
- The Best Practices enables Do Not Display Last User Name in Logon Screen, but the template lets it display. For an office environment where everyone sits at the same desk most of the time and the userid naming convention is well known, let's give the users the convenience of having the userid prefilled.
- The template doesn't stipulate a Message Title or Message Text for logons, but Best Practices does. We'll do a logon message.
- Number of Previous Logons to Cache: Best Practices: 0; template: 10. How about 2? That will get people over momentary network glitches without too much risk, unless the concern is over crackers recovering cached credentials from the hard disk.
- Rename Administrator and Guest Accounts: Secure DC template leaves these undefined; we'll agree with Best Practices and rename them.
- Smart Card Removal Behavior – doesn't matter- we haven't implemented them (yet.)
- LAN Manager Authentication Level – the template calls for NTLM only; I prefer the Best Practices- Send LM & NTLM, use NTLMv2 if negotiated. It's more flexible.

In browsing through all these settings, I note that the IIS anonymous users IUSR_machinename and IWAM_ machinename have various rights assigned to them, so on Domain Controllers, I think these accounts will get disabled.

Under Event Log, we'll make all the logs huge (at least 10 megs) and set all the retentions to 'as needed.' There's no need to scrimp on logging space in these days of huge hard disks.

Finally, we'll disable the User portion of the GPO.

Before these guys go into production, we'll test as much as possible to make sure the settings don't mess up the network.

Member Server Group Policy will be similar to DC, except we'll begin with the Secure Workstation template. This template seems to vary from the DC template mostly in the area of User Rights Assignment under Local Policies – this area is heavily defined for DCs, completely undefined for Workstations. We'll undefine the Account Policy stuff, delete the Administrative Templates, and disable the user portion. And we'll set up the same compromises between the template and the Best Practices as we did on the DCs, with one exception. We'll give the Application Event log an extra large size (20 megs) to provide plenty of space for error messages the applications running on these servers may generate while they're being tested and straightened out prior to production. Testing and production monitoring may lead to further policy tuning going forward. We'll also limit the Manage Auditing and Security Log User Right to Administrators, like on DCs. Anything you can do to secure logging is important for tracking down problems and catching intruders.

IT Workstation Policy will start out just like the servers – import the secure workstation template, undefine the Account Policies that are already set at the Domain level, reconcile the settings with the SANS Best Practices, delete the Administrative templates, and disable the User Configuration portion. As the IT gang gets the hang of GPOs, they can argue about and tweak their policy till the cows come home, without messing up anyone else.

That leaves the Staff Workstations OU and the Laptops and Deploy OUs nested inside it.

Workstation Group Policy will start off the same as the IT Workstations – complete with Best Practices review and all the other tweaks. We'll restrict management of auditing and security logs to Administrators. Going forward, we can fine tune policy for staff workstations and laptops at the appropriate level, without worrying about conflicts with other types of machines.

I want most of the users to get their My Documents folders redirected to a share on the net. This needs help from Offline Folder Synchronization to work well for laptops, though. So, the Laptop GPO will have settings for autocaching the home share, and that's it. This probably means we'll have to keep the User Configuration node enabled, and use Loopback. As this is written, I'm still working on it.

Deploy's GPO will be empty most of the time, except when we want to do big software deployments. To set up a deployment, right click on the Software Installation extension found in Software Settings under the Computer Configuration node. The details of this process are fairly involved and beyond the realm of this document.

Group Policy for Users

This is probably the area everyone thinks of when Group Policy is mentioned – doing all those UI tweaks and lockdowns we used to do with NT System Policy and TweakUI. GIAC doesn't need to turn its computers into dumb terminals, though – at least not for the most part. We'll save the Draconian lockdown routine for people who end up in the "Restricted" OU.

First off, as mentioned earlier, the IT Staff OU exists largely to exempt IT people from User Configuration Policy. They won't get any, other than a login script that's set up for them.

The Staff OU will get a general purpose login script derived from the old NT 4 one. It will map drive shares and help set up the anti-virus software. It will also get My Documents redirected to a home share on the net, in a subfolder called %username% that the user will have exclusive full access to. This is the default when you set up Basic Folder Redirection.

To set basic redirection up, go into the User Configuration node of Group Policy, then open Windows Settings>Folder Redirection, and choose a folder to redirect. Right click on the folder icon, and choose Properties. On the Properties dialog, choose Basic from the Setting drop down menu. Enter the share name in the Target folder location field in UNC format, and include the %username% variable so that everyone gets their own subfolder. It should look something like this:

\\servername\sharename\%username%\My Documents

Then, hit the Settings tab and review the selections. Generally, the defaults work, but you might wish to change 'Policy Removal' to put the folders back on the local drive if the policy is removed, and you also might leave My Pictures on the local hard disk to avoid filling up the share with big graphic files.

There's a good basic write-up on folder redirection in the Directory Services Exam Cram.[12]

Login Scripts and Folder Redirection are the only pieces of the Windows Settings child node that we'll worry about for the Staff OU. Next we'll look at the Administrative Templates node.

Under Windows Components>Microsoft Management Console, we'll eliminate access to practically everything – no author mode, and a very short list of allowed snap-ins – Disk Defrag and Shared Folders come to mind. Most users couldn't care less about snap-ins, and those who do usually produce support calls.

Under Start Menu & Taskbar, we might do Remove Network & Dialup Connections from Start Menu, and enable Add Logoff to the Start Menu. Add Logoff is almost mandatory on server consoles to keep people from accidently rebooting the box when they're trying to logout. It's not so important on clients, but it is a convenience. We will definitely Disable and remove links to Windows Update- IT needs to be in charge of updating desktop operating system components, or we'll slowly develop a fleet of unique and flaky machinery.

Under Desktop, we probably don't need to do anything.

Under Control Panel, we can either Hide specified control panel applets, or Enable only specified control panel applets, depending on how many are involved. In most cases, it would probably be best to disable only Administrative Tools, Licensing and System. Ordinary users don't care about these things, and fiddlers just generate calls with them.

Under Control Panel>Desktop, we should Activate screen saver, Password protect screen saver, choose an initial Screen saver executable name, and set a Screen Saver timeout of

10 minutes. This is to protect user workstations when they're left unattended and logged in during lunch, meetings, et cetera, and it's not as obnoxious as forcibly logging users off after a given period of inactivity.

Under Network, we probably don't need to do anything, unless we get tinkerers messing with their systems. Then we could tighten down the Network settings in the Restricted OU and add those folks to it.

Under System, it would be prudent to Disable registry editing tools. This is another thing most users don't need, and we don't need them having access to them.

Policy for Restricted users, and who belongs in that OU, can be determined over time. As it's nested in the Staff OU, Restricted users will still get all the policy we set up for Staff. The main idea here is to protect that set of users who get themselves into trouble, by fencing them off from 'dangerous' system features. In doing so, we're also protecting ourselves from unnecessary support work, without limiting people who can use the extra freedom appropriately.

Service Accounts is another OU whose policy can be determined over time as we test various applications and services and determine what their service accounts need to have to function properly. Given that such accounts tend to be few in number, it's no big deal to set them up directly on their properties pages for things like 'user cannot change password' (if a service account tried that, you've got a security issue) and 'password never expires' (when one does, it typically kills the associated application.) It's still a good idea to provide a self-documenting, dedicated can to throw these oddball accounts into, where we can save them from everything we set up for general user accounts.

Chapter 5

Miscellaneous Security Topics

Necessary Odds and Ends

Many things needed to secure a Windows 2000 network got discussed while we laid out the proposed physical network in Chapter 2, so we won't go back over them here. There are some remaining things that we need to talk about, though.

First off, it goes without saying that there will not be any FAT partitions anywhere on the network except for on floppy disks! Everything will be NTFS v. 5. You don't get any security with a FAT or FAT32 file system. You can control and audit access to file system objects with NTFS. This is especially important for servers; even more so for publicly accessible ones like our web server.

Second, we need to work toward getting Everyone out of the "Pre Windows 2000 Compatibility" group. It's not something we can do today, but once all the applications are tested and the mail server is migrated, it needs to happen.

Intrusion Detection is too big a topic to go into detail on here, but suffice it to say that host based intrusion detection is an important part of keeping tabs on DCs, web, mail and application servers, along with auditing Event and IIS logs.

Log Management

That brings us to the topic of logs and what to do with them.

We've set up our servers to do a great deal of logging. Event Log on our DCs keeps separate logs for Application, Security, System, Directory Service, DNS Server, and File Replication Service. The web server generates IIS logging. The routers and firewalls are capable of sending events via syslog. Logging is step one of keeping track of things. Step two is protecting logs: archiving them, and working to prevent intruders from altering logs in order to hide their tracks. Step three is developing a method for gleaning need-to-know information from reams of logging data.

One of the prime ways to keep intruders from destroying logs is to send logging data to a secure centralized logging server. There is more than one way of doing this, but I want to briefly describe one way it can be done.

Unix people are familiar with syslog, a generic logging service that collects logged events from client machines and programs on UDP port 514 and writes them to a file. A daemon (background program, similar to a Windows Service) typically called *syslogd*, listens on this port for inbound log entries. Several programs that implement this functionality for Windows are now available. SL4NT (http://www.netal.com) and WinSyslog (http://winsyslog.com) are two of them.

Most firewalls and routers will send syslog natively, so that's no problem. To get Windows logs into syslog, you need a syslog client that will capture Windows Event logging and send it to a syslog server. Two programs that do this are ntsyslog (http://www.sabernet.net/software/ntsyslog.html) and EventReporter (http://www.eventreporter.com.) Norberg's book has a section that discusses syslogging in the Windows environment.[13]

No law says you can't continue to manage Event Logs with the native Event Log viewer or other Microsoft tools, but now you've got another copy of them squirreled away elsewhere on your network.

IIS Logs are generated by IIS itself and stored as text files, usually in a separate file for each day in %systemroot%\system32\logfiles\w3svc*n*, where *n* is the ordinal number of the website, as IIS reckons it. You could use a variety of methods to copy these across the net periodically, such as a scheduled batch file (but it wouldn't end up in syslog's files, just in a directory.)

Once you've got all this log collecting on a hard disk somewhere, you can copy it to tape or burn CDs for archival purposes. Some people set up syslog to write its files to write-only media, making it harder for crackers to mess with them.

The big payoff to all this, besides the security aspects of saving logs in more than one place, is the ability to go surfing through all the log data for 'interesting' entries that may indicate system problems or intruder activity. A variety of products are available to monitor Event Logs in realtime and send you alerts (including some of those mentioned above) but usually this is done on a server-by-server basis. Having all the day's logs in one place gives you a way to spot things that are happening *around* your network over time. To do this, you gotta do two things: get familiar with what events qualify as 'interesting', and learn a bit of scripting (or buy a product to crank the logs for you.) Either VBScript or Perl work great for this – anything that will work with regular expressions. Regular expressions are a powerful but fairly non-intuitive way of describing and searching for text patterns, originally developed in (where else?) the Unix world. SANS Securing Windows 5.5 curriculum is a good start in learning VBScript and its security applications. For Perl, you can't beat Learning Perl (the 'Llama Book') and Programming Perl (the 'Camel Book') by O'Reilly & Associates, or try http://www.perl.com (an O'Reilly site) and http://www.perl.org. In fact, there's even a Learning Perl on Win32 Systems book from O'Reilly.

Well, that's it for now. Security is a never ending activity, but this paper ought to provide plenty to start with! Thanks for reading.

Appendix **A**

References

and Endnotes

Endnotes

1. Norberg, pp 32 – 101.
2. Brelsford, http://www.windowsitlibrary.com/Content/329/14/1.html#1.
3. Savill, http://www.windows2000faq.com/Articles/Index.cfm?ArticleID=21331&Key=Windows%202000%20Service%20Pack%202%20%28SP2%29
4. Microsoft, "Deployment Planning Guide," p 313.
5. Willis, et al, p 165.
6. Microsoft, p 297.
7. Microsoft, "Distributed Systems Guide," p 1234.
8. Microsoft, pp 1238-1239.
9. Microsoft, p 1240.
10. Willis, et al, p 193.
11. Schein, p 310.
12. Willis, et al, pp 200-201.
13. Norberg, pp 160-163.

References

Norberg, Stefan. "Securing Windows NT/2000 Servers for the Internet." Sebastopol: O'Reilly & Associates, Inc., 2001.

Brelsford, Harry. "History and Role of Service Packs." Microsoft Windows NT Secrets: Option Pack Edition. April 1999. Windows IT Library. URL: http://www.windowsitlibrary.com/Documents/Book.cfm?DocumentID=329

Originally published in book form by IDG Books, 1999.

Savill, John. "Q. How do I create a bootable Windows 2000 CD-ROM with a service pack slipstreamed?" June 4, 2001. John Savill's Windows NT/2000 FAQ. URL: http://www.windows2000faq.com/Articles/Index.cfm?ArticleID=21331&Key=Windows%202000%20Service%20Pack%202%20%28SP2%29

Willis, Will, et al. "MCSE™ Windows® 2000 Directory Services Exam Cram." Scottsdale: The Coriolis Group, LLC, 2000.

Microsoft Corporation. "Microsoft Windows 2000 Server Resource Kit." Redmond: Microsoft Press, A Division of Microsoft Corporation. 2000.

Schein, Phillip G. "MCSE™ Windows® 2000 Security Design Exam Cram." Scottsdale: The Coriolis Group, LLC, 2000.