Global Information Assurance Certification Paper

GCNT PRACTICAL VERSION 3.0

LuckyBoyFortunes.Com, a GIAC Enterprise Corporation

Author: Nate Morin

December 2001

Table of Contents:

Introduction

In only their second year, our young LuckyBoyFortune is having a banner year. It seems the demand for fortune cookie sayings is at an all time high, some might even say fortune cookies are the new .coms. Of course the naysayers will whisper of improper business practices and corruption but we at LuckyBoyFortune believe they're all just jealous of our success.

We will admit that we have had an incredible run-up from our first year's results, but this can be directly attributed to our eloquent business plan and our wonderfully sophisticated and beautifully crafted website LuckyBoyFortune.com. Of course our web presence features all the latest web technologies and the overly complex user interfaces necessary in today's market.

To be completely honest; we feel there is no connection between our recent acquisition by the Gino's Fine Jewelry, Furrier & Electronics Corporation and our new found success. Furthermore it was pure coincidence that one of our fortune cookies happened to contain the winning numbers for the Tri-state Lottery's $148 million dollar jackpot. In fact it's only logical for one surmise that Gino's brother in-law would have a greater than average chance of receiving this fortune, as he is a silent partner in one of our largest fortune cookie customers.

Flush with new cash our LuckyBoyFortune decides they absolutely need to build themselves a highly secure information infrastructure to safeguard their competitive advantage.

Network Design

Timing could not have been better for LuckyBoyFortune's IT director as he had timed his budget request immediately following his return from the Boston SANs conference where he attended the Track 5, Securing Windows course. In an even greater stroke of good fortune, Gino our new CEO, had just seen a story on GNN on the destruction caused by the nimda worm and the overall sorry state of network security in corporate America. Armed with a ridiculously large budget for such a small enterprise, our IT director plans the LuckyBoyFortune network infrastructure.

Fresh from the conference, the IT director knew he was in a unique position of being able to purchase any combination of hardware and software he wanted. He also knew that the most effective network security design is a cradle to grave program. With this in mind, he decided to completely redesign LuckyBoyFortune's hardware

infrastructure by purchasing all new equipment from backbone equipment to servers to desktop clients. The program must feature a defense in depth with a combination of hardware and software solutions. While the desktop configuration management and security would be implemented and enforced using Microsoft's Active Directory and Group Policy.

From the border gateway router down to the switch supporting the desktop clients, here are the solution we decided upon. (See figure 1)

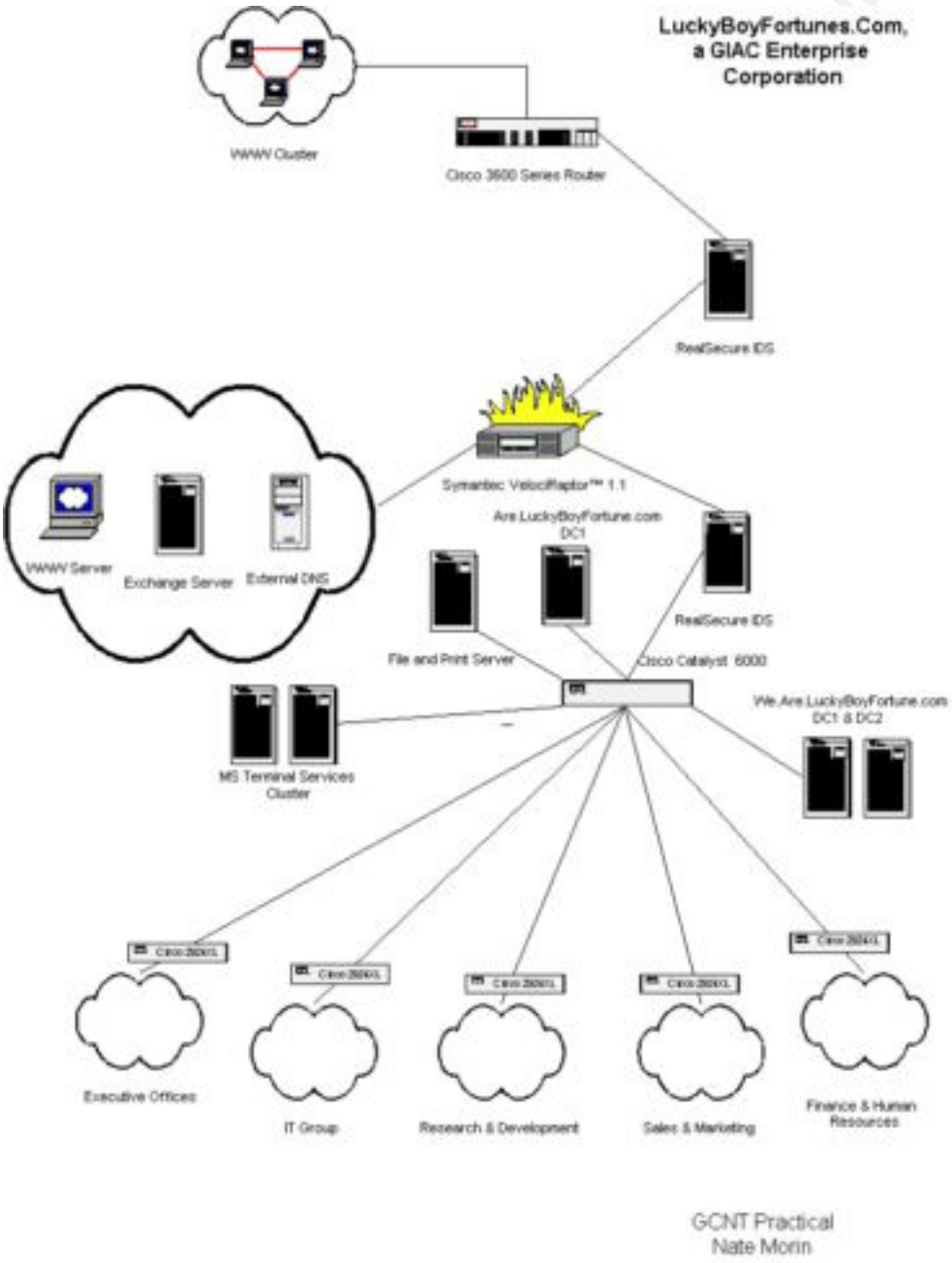


Figure 1: Network

Border Gateway Router: We choose a Cisco 3600 Series Router to serve as our border gateway router. This will provide us the scalability we may require as our business grows by supporting features such as: multiple T1/E1 links, VoIP, VoFP, ATM and dial up services.

Outside Firewall IDS: To accurately measure the type of traffic that is hitting our firewall we choose to place a **RealSecure Network Sensor** on both the inside and the outside of our firewall. RealSecure Network Sensor monitors the network traffic for attacks or other suspicious activity. It can then terminate the connection, send email or pager alerts, record the session, reconfigure select firewalls or take other, user-directed actions. This will allow us to quantify the outside threat as well as the threat that is making it past our firewall. We have purchased a Dell PowerEdge 2550 Server the IDS.

Firewall: On the inside of the Real Secure Network Sensor we have placed a Symantec VelociRaptor 1.1 firewall appliance.

> **Symantec VelociRaptor™ 1.1** is an integrated hardware and software firewall/VPN appliance that employs full-inspection technology to provide a fast and secure connection to the Internet, delivering enterprise-class network security. The single-rack unit high (1RU), plug-and-protect appliance ensures complete control of information entering and leaving the network with data inspection technology that filters traffic and integrates application level proxies, network circuit analysis, and packet filtering into the gateway security architecture. To bar access to private networks and confidential information, Symantec VelociRaptor 1.1 applies full-inspection scanning techniques that ensure that data is validated at all levels of the protocol stack, including application proxies. [1]

Inside Firewall IDS: On the inside of the Symantec VelociRaptor we placed another **RealSecure Network Sensor** to monitor the traffic on the inside of the firewall. We have purchased a Dell PowerEdge 2550 Server the IDS.

Top Level Switch: Inside the second IDS we place a **Cisco Catalyst 6000** switch to handle routing duties within our network. Some of the Catalyst 6000 features include: gigabit scalability, support for quality of service bandwidth allocation, support for VLANs, and load balancing across Layer-3 paths.

Business Unit Switch: Each of the three business units: Research and Development, Sales and Marketing and Finance and Human Resources will get a combination of Cisco 2924XL switches. This switch features: A Web-based interface, Cisco Visual Switch Manager, support up to 64 port-based VLANs, and 1000BaseT Gigabit Interface Converter (GBIC) to provide Gigabit connectivity between critical servers or backbone equipment.

[1] Symantec Corporation

Servers: Microsoft's Windows 2000 Advanced Server has been chosen for the Domain Controllers, Terminal Services Servers, Internet Information Server (IIS), Exchange Server and Domain Name Server. We plan to leverage Microsoft's Active Directory (AD) and Group Policy features to further enforce the defense in depth we have built with the hardware of our network equipment. In general all servers are running the same basic security configuration of Service Pack 2 and the following hotfixes [2]: Not all fixes were applied to all servers nor is this an exhaustive list of all hotfixes applied to each of the different servers in our network configuration. For a specific list of applicable hotfixes per server visit Microsoft's Security Bulletin Search [3].

MS01-052 : Invalid RDP Data can Cause Terminal Service Failure

MS01-046 : Access Violation in Windows 2000 IRDA Driver Can Cause System to Restart

MS01-043 : NNTP Service in Windows NT 4.0 and Windows 2000 Contains Memory Leak

MS01-041 : Malformed RPC Request Can Cause Service Failure

MS01-040 : Invalid RDP Data Can Cause Memory Leak in Terminal Services

MS01-037 : Authentication Error in SMTP Service Could Allow Mail Relaying

MS01-036 : Function Exposed via LDAP over SSL Could Enable Passwords to be Changed

MS01-031 : Predictable Named Pipes Could Enable Privilege Elevation via Telnet

MS01-025 : Index Server Search Function Contains Unchecked Buffer

MS01-024 : Malformed Request to Domain Controller Can Cause Memory Exhaustion

MS01-022 : WebDAV Service Provider Can Allow Scripts to Levy Requests as User

MS01-013 : Windows 2000 Event Viewer Contains Unchecked Buffer

MS01-011 : Malformed Request to Domain Controller Can Cause CPU Exhaustion

MS01-007 : Network DDE Agent Requests Can Enable Code to Run in System Context

MS00-079 : HyperTerminal Buffer Overflow Vulnerability

MS00-077 : NetMeeting Desktop Sharing Vulnerability

[2] Microsoft Corporation

[3] Microsoft Corporation

Domain Controllers, RealSecure Network Sensors and External DNS Server: Our network design includes three Domain Controllers, one for the root domain, and two for child domain. While our network of 100 users could very easily be supported by one DC (diagram 1) the value added by having a root domain in our AD structure and the security of having a second DC in our child domain more than justices that added cost. All Domain Controllers store a writable version of the Active Directory Database. With the implementation of AD there is an even greater need to ensure the physical security of an organization's Domain Controllers.

At LuckyBoyFortune we have separated our 3 Domain Controllers into three separate rooms. All rooms have the following security devices and measures in place: Solid walls, ceiling, and floor with a single metal door and a substantial lock. The metal door that has a smartcard reader that logs the users name and the time that user entered the room. All users must swipe in and out of the server room. Once all users that have swiped in, swipe out, the motion sensor alarm in the room is activated. Additionally, the room is windowless, temperature controlled, has a dry fire protection system.

The following hardware configuration was selected:

(5) Dell PowerEdge 2550 Servers featuring:
1 GHz PIII Processor
1 GB SDRAM
(2) 18GB, 1" Ultra3 SCSI 10K RPM Hard Drive in Raid 1 configuration

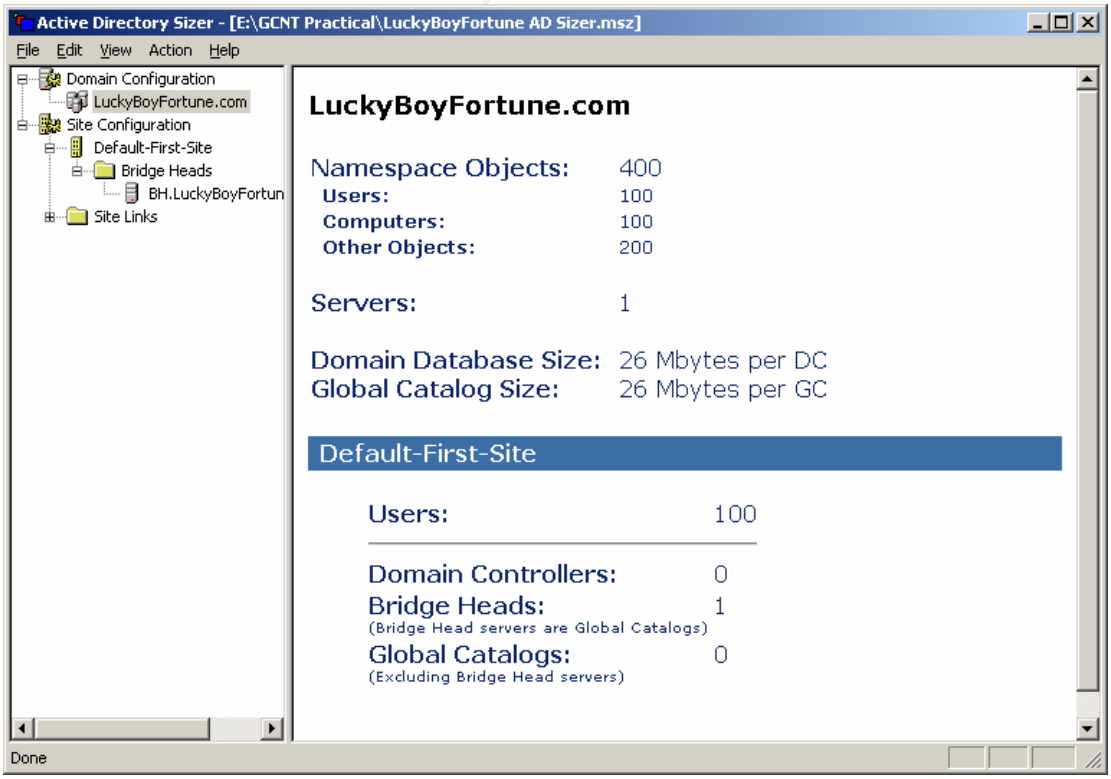


Diagram 1: Microsoft Active Directory Sizer Tool

Microsoft Terminal Services: We have chosen to run Microsoft Advanced Server providing desktop Windows 2000 Professional desktops and applications. To aid in accessing our needs we used the Dell Powermatch for Terminal Server application (diagram 2). These two Dell Servers featuring Microsoft Advanced Server are running network load balancing to provide an additional level of performance and redundancy for the clients. The implementation of Terminal Services will drastically lesson administrative requirements in maintaining the security configurations of the client machines.

The following hardware configuration was selected:

(2) Dell PowerEdge 4400 Servers featuring:
1 GHz Xeon Processor
512 MB SDRAM
(4) 36GB, 1" Ultra3 SCSI 10K RPM Hard Drive in a Raid 5 configuration

Diagram 2: Terminal Server Configuration

Internet Information Server (IIS): Our website, LuckyBoyFortune.com is hosted on a Microsoft Windows Advanced Server 2000 machine with IIS 5.0. The hardware chosen to support our website was Dell PowerApp Web 120. The PowerApp 120 is an

appliance optimized to provide reliable and robust webpage hosting while minimizing administrative overhead. This hardware will enable us to quickly react when our owner chooses to exercise his desire to enter to online gaming business. While this device will not support us indefinitely, it will allow us to support our current web operations with some definite expandability built in.

The following hardware configuration was selected:

(1) Dell Power App Web 120 featuring:
1.13 GHz PIII Processor
512MB SDRAM,
(4)18GB, 1" Ultra3 SCSI 10K RPM Hard Drive in a Raid 5 configuration

Exchange Server: Prior to purchasing the hardware to host our Microsoft Exchange 2000 Server, we again ran one of those handy tools to help in gauging our hardware requirements, the tool chosen for our Exchange 2000 hardware was the Microsoft Exchange 2000 Hardware Sizer (diagram 3). In the interest of minimizing the complexity of our onsite and purchased hardware support, we elected to once again purchase a Dell PowerEdge. Bundled with the PowerEdge was a PowerVault 120T External 20/40GB DLT-4000 Autoloader Rack-Mount backup solution. This device will be used to perform backups on not only the Exchange Server but also the File Server, Web Server, and the Domain Controllers.

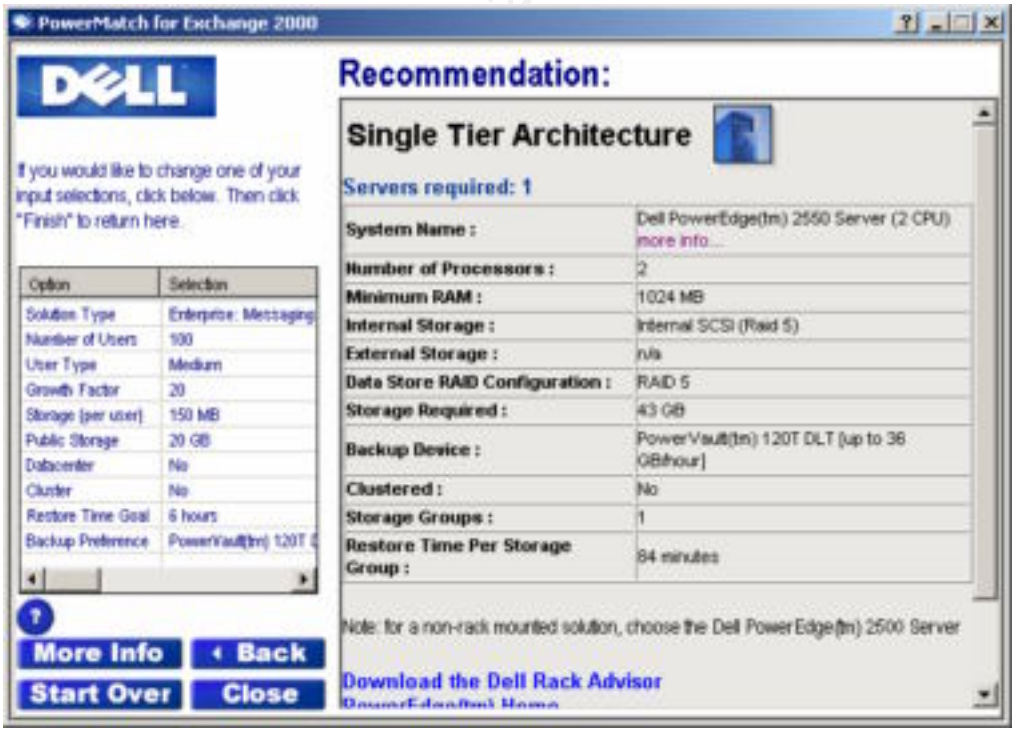


Diagram 3: Exchange 2000 Server Configuration

The Active Directory and Group Policy structure will discussed in much greater detail in the following sections. The resulting hardware and network design could be seen as overkill. We believe security is expensive, so how secure can we afford to be? Alternate designs could possibly provide adequate security with cheaper products such as lesser model Cisco equipment or Microsoft's Internet Security and Acceleration Server 2000 (ISA) but we feel the overall supportability and expandability of our design is more appropriate.

Recently our purchaser, Gino's Fine Jewelry, Furrier & Electronics Corporation, has expressed in interest in expanding our business into the online gaming industry. He sees this as a highly lucrative and still fairly undeveloped market sector. To ensure the network infrastructure can support this planned growth we have purchased hardware which is vastly expandable.

Clients: We haven chosen a mix of Windows 2000 Professional and Windows 2000 Terminal Services thin clients to support our users.

The cost for the client machines has not been calculated as we are still gathering those requirements. The majority of the clients will eventually be thin clients to add to the overall security posture of our organization and to lessen the administrative overhead. Those who travel frequently will be given W2K laptops on which they can synchronize their files for offline usage prior to their trips. The following hardware and software was purchased to support of the network design:

Quantity	Device	Approximate Cost
1	Cisco 3600 Series Router	$ 4900.00
1	Cisco 2924XL Switch (5 Pack)	$ 9900.00
1	Cisco Catalyst 6000 Switch	$ 10126.00
1	Symantec VelociRaptor 1.1 (500 Nodes)	$ 7100.00
2	Symantec VelociRaptor 100 User VPN	$ 1600.00
2	Internet Security Systems (ISS), RealSecure Network Scanner single user	$ 8878.00
6	(2) IDS, (1) DNS, (3) DC: Dell PowerEdge 2550 Servers, 1 GHz,, 1 GB SDRAM, (2) 18GB 1" Ultra3 SCSI 10K RPM Hard Drive	$ 30000.00
2	(2) Terminal Servers: Dell PowerEdge 4400 Servers: 1GhZ Xeon 512 MB SDRAM, (4) 36GB 1" Ultra3 SCSI 10K RPM Hard Drive	$ 24866.00
2	(1) Exch , (1) File & Print Server: Dell PowerEdge 4400 Servers Dual 1 GHz,, 1 GB SDRAM, (4) 36GB 1" Ultra3 SCSI 10K RPM Hard Drive	$ 20168.00
1	(1) Web Server: Dell Power App Web 120, 1.13 GHz, 512MB SDRAM, 18GB Ultra3, 1 IN, 10K RPM, SCSI Hard Drive	$ 3180.00

Total Estimated Cost for Network Hardware $ 145,644.00

DNS Design

DNS is an integral and mandatory addition to any Active Directory integrated domain. Client systems within the AD domain query the DNS server for the location of the Domain Controller they want to log on to. Use of the Windows 2000 DNS server is not mandatory since any DNS Server supporting Service Location Resource Records (SRV RRs) and Dynamic Update (RFC2136) will provide the necessary support to Windows clients. Although other DNS services are available, it is recommended to stick to the Microsoft implementation of DNS as DNS can be integrated into the Active Directory service, and can take advantage of the multi-master replication features of Windows 2000. Additionally the integration of DNS into Active Directory lessens the workload of the administrator eliminating the need to plan or maintain an additional replication scheme for DNS. Other additions to Windows 2000 DNS include incremental zone transfer, support for dynamic updates and the ability to configure and access control list for each DNS record.

Both Domain Controllers within the child domain LuckyBoyFortune will run DNS. Access from the internet to internal DNS servers will be blocked by our Raptor Firewall. The external DNS server will only host the absolutely necessary records for the Exchange server and the Web server. The internal DNS servers will forward all external DNS resolution requests to our external DNS located in the screened subnet. Some additional steps we have taken to harden our DNS infrastructure include [4]:

- Configured ACLs on critical DNS records: Exchange server, Web server, Domain Controllers, IDS Servers, Term Servers, and the File & Print Server
    - Increase security by assigning specific users or groups access
- Use the QueryIpMatching registry value to help prevent cache poisoning
- Disable zone transfers on internal DNS servers (not needed since zone transfers are performed during AD replication

Active Directory Design

Once the proper hardware is in place we could focus on our Active Directory Design. Much like the philosophy we used in building our network structure, we tried to find a balance between security, ease of administration and expandability when building our AD structure. Although LuckyBoyFortune is currently a small corporation operating from a single site we have aspirations of growing the business to multiple locations and even possibly multiple countries over the next few years. Additionally LuckyBoyFortune's new owners have been extremely successful at acquiring other ailing corporations at truly rock bottom prices.

Since LuckyBoyFortune already had a registered DNS name: LuckyBoyFortune.com, we choose to leverage our existing name recognition by continuing to use this namespace. Starting at the top of the AD model we designed a single site with a single forest with a single tree. On this tree we placed two domains: Our root domain, LuckyBoyFortune and our child domain, Corp.LuckyBoyFortune.com. Within the Corp.LuckyBoyFortune.com domain we have created following 5 Organization Units (OU) (figure 2): Executive Group OU, Research & Development OU, IT Group OU, Sales and Marketing OU, and the Finance and Human Resources OU, as well as some subordinate OUs we'll discuss later:

[4] Fossen (111-112)

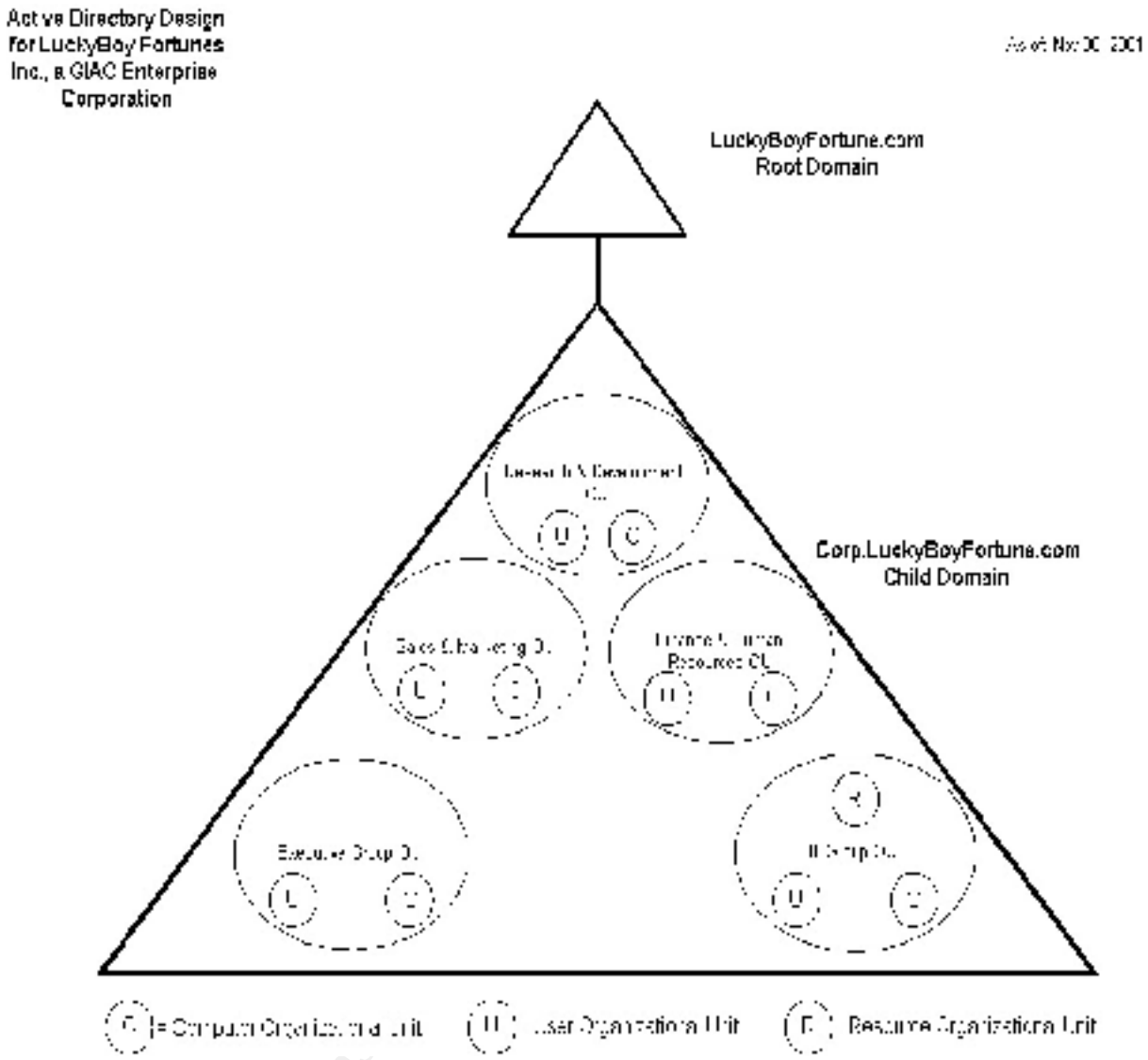


Figure 2: Active Directory Design

A two domain model was selected for our organization as a compromise between manageability and expandability. The top level forest root domain: LuckyBoyFortune.com only requires an additional commitment of one Domain Controller to serve as our place holder domain and allow us to easily add more child domains should it later become necessary. No objects were added to the root domain and no plans exist to ever add any there.

We choose a single child domain to ease the administrative burden and because it can very effectively support our current organizational structure. With only one domain we have no inter-site replication issues, no complications from GPOs spanning domains, a reduced requirement for Domain Controller hardware, and no need to ever move objects between domains.

Organizational Unit Design:

The design scheme for our five departmental OUs: (Executive Group, Research & Development, IT Group, Sales and Marketing, and the Finance and Human Resources) was based partially on our desire for decentralized administration of the resources within the individual departments and partially on our need to apply different user and system configurations based on the unique needs of the departments (diagram 4).

Each department has dedicated Tier I and Tier II automation support personnel. Each department, other than the IT Group, has two Tier I support personnel and one Tier II support person. By utilizing the delegation of control wizard we were able to assign specific administrative duties to each group of support personnel. We have assigned our IT support personnel to their respective groups based on their experience. Those with the most experience will be granted the greatest degree of control over the OU.

The Tier I personnel provide immediate Help Desk type call resolution for troubleshooting and are able to: reset passwords on accounts of those in the section. The one Tier II individual in each section is able to additionally: create, delete and manage user accounts, read all user info, and modify the membership of a group, and manage the hardware resources within their OU. The Corporate IT Group consists of one tier I person, two Tier II personnel and two tier III engineers who are additionally able to: create, delete, and manage groups and manage group policy links.

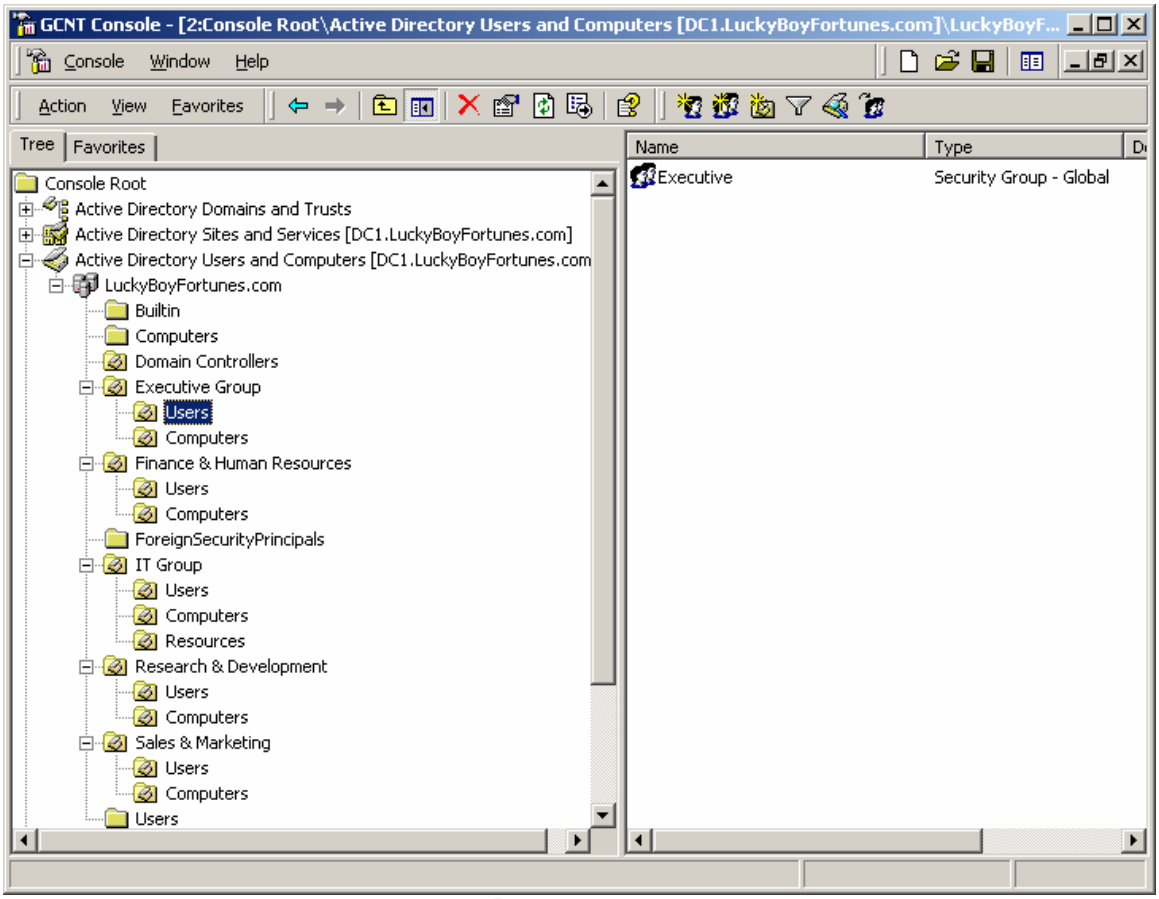


Diagram 4: Organizational Unit Design

By creating the Computer and User sub OUs we are able to easily differentiate the application of Group Policy Objects (GPOs) between the users and the computers within a department. These sub OUs additionally allow us to apply the same GPO to computers or users across multiple departments, assuming they have similar operational and administrative requirements. An additional consideration in creating OUs at the department level was the ability to publish or assign unique software packages by linking specific GPOs to OUs. For instance, we could assign Microsoft Publisher to the Sales and Marketing OU by using the following steps:

- Open: AD Users and Computers
- Select the Sales and Marketing OU > Computers
- Right-click and choose > Group Policy tab
- Add Sales and Marketing GPO (previously created)
- Select > Edit to expand GPO settings
- Choose > Computer Configuration > Software Setting
- Right-click Software Installation
- Select > New > Package
- Select Microsoft Publisher msi. package

To further simplify administration of domain resources we have created Global Security groups within each user sub OU. These Global groups will allow us to easily control access to resources by adding the required Global groups to the Domain Local group where the resource resides. Access control lists can be applied to the resource and we can add or remove access based on Global group membership.

We have chosen to place users into groups created within the departmental OUs where they work. This was done to provide faster and more personalized service as the Tier I and Tier II support personnel will be given control over those departmental group user accounts. Since we are also using these departmental group accounts to access sensitive materials throughout the company, we have additionally created manager groups within each department.

Using this design the Tier I and Tier II support personnel within the department can provide the daily support the Finance & Human Resources Department requires by managing the Finance & Human Resources Users Group. While they have full control over the Users Group: reset passwords on accounts, create, delete and manage user accounts, read all user info, and modify the membership of a group, and manage the hardware resources within their OU they can only unlock user accounts of the Managers Group. The Finance & Human Resources Managers Group is managed by the Tier III support personnel from the IT Group as are all the Departmental Managers Groups. This separation of administrative control sacrifices some convenience to provide an additional level of security for the company's more sensitive shared network resources. As an added level of security we audit changes to group membership and access to sensitive files and folders to ensure an administrator doesn't add themselves to a group, download the payroll records, then remove their account from the higher level group to avoid detection.

Since our network is quite small and we have only nested OUs a couple deep we do not expect any performance degradation based on our AD Design. Now that we have the network hardware and AD structure in place we can move on to the application of Group Policies to provide the final layer of our Secure Windows 2000 Infrastructure.

Group Policy

With the introduction of Windows 2000, Windows administrators around the world were given a very powerful and effective tool to aid them in their configuration management woes. The foundation for this tool is Microsoft's Group Policy. Along with Windows 2000 came Active Directory, with AD administrators are able to leverage Group Policy to assist them in applying and maintaining the required system and user settings for the security of their network. The proper implementation of Group Policy can drastically improve the resulting security of a Windows network by ensuring the reliable application of predefined and customizable set of system and user account configurations.

Group Policy can only be applied to Windows 2000 clients. Previous to Active Directory and Group Policy, administrators of Windows NT 4 networks could have used System Policy Editor (Poledit.exe) to assist them in configuring some of these settings but it lacked the refinement of the Microsoft management Console (MMC) and the Group Policy Editor (GPE). Administrators of Windows 95 and 98 needed to create OS specific configuration policies: (config.pol), while NT 4 administrators needed to create their own OS specific configuration policies: (NTConfig.pol). Additional configuration management options prior to Windows 2000 included Microsoft System Management Server (SMS) and some other 3rd party applications such as St. Bernard's Update Expert and Computer Associates Unicenter line of products. The Windows 2000 Server family gives administrators a true enterprise management solution without the added expense of procuring and managing another external application.

After installing the Security Templates snap-in from the MMC administrators can import predefined security templates and then edit these templates with the GPE. Many outside organizations have spent considerable effort to develop even more secure configurations than Microsoft offers with their predefined security templates. It is definitely worth the effort for security conscious administrators to research what templates are available prior to settling for one of the predefined templates.

In establishing our Group Policy settings we are starting with the Default Domain Policy and working down through our other servers to the lower level computers and groups. This allows use to apply increasingly secure configurations at the lower levels where we need the most granularity of control. It also ensures that our most restrictive Group Policy setting are not over written by a lower level Group Policy linked to an OU. By default, GPO settings are applied in the following order: local machine GPOs, site based GPOs, Domain based GPOs, and specific Organization Unit GPOs. The GPO that is applied last is the resulting setting unless a higher level administrator has enabled the No Override option on the GPO link for a particular setting. Depending on the level of control delegated to the OU administrators, they may be allowed to enable the Block Policy Inheritance feature within their OU GPO settings to resist the application of settings created at higher level from being applied to their OU. Ultimately, higher level administrators can always override lower level ones if they select the No Override option.

It is critical that organizations clearly identify those settings that are mandatory for all users and systems in the organization. Some settings that are generally enforced from the top levels through the use of the No Override feature can be found under the GPO > Computer Configuration > Security Settings > Account Policies. Administrators should be careful when using the No Override and Block Policy Inheritance options as they will make it exceptionally difficult to troubleshoot any problems associated with the applications of GPOs.

In designing the GPO structure for LuckyBoyFortune the we will not select the No Override option on any of our Group Policy Objects. Since all the GPO designers work for the IT support staff in our small company we are fairly certain the minimum

standards can be maintained without the additional complication of enforcing the No Override function. As an additional level of security we have chosen exclude the publicly accessible web server from our domain. We will configure the security settings of the web server manually as the ease of administration of this machine is over shadowed by our need to apply a greater degree of security to this system. To speed the application of this domain wide GPO we have disabled the User Configuration Settings so they do not process at logon. To disable application of the User Configuration Settings:

- Open the GPO to be edited
- Right-click on the console root (LuckyBoyFortune Domain Wide GPO [DC1.LuckyBoyFortune.com] Policy)
- Click Properties, ensure the Disable User Configuration settings is selected, and then click OK

Windows 2000 comes with two predefined GPOs: Default Domain Controller Policy and Default Domain Policy. For the LuckyBoyFortune network we have chosen to initially create three additional GPOs for the following departments: Research and Development, Finance and Human Resources and the resources sub OU within the IT Group OU. First we will examine the modifications to the two default GPOs (Default Domain Controller Policy and Default Domain Policy) and then we will discuss the additional security and operational requirements the dictated the creation of the additional three OU GPOs.

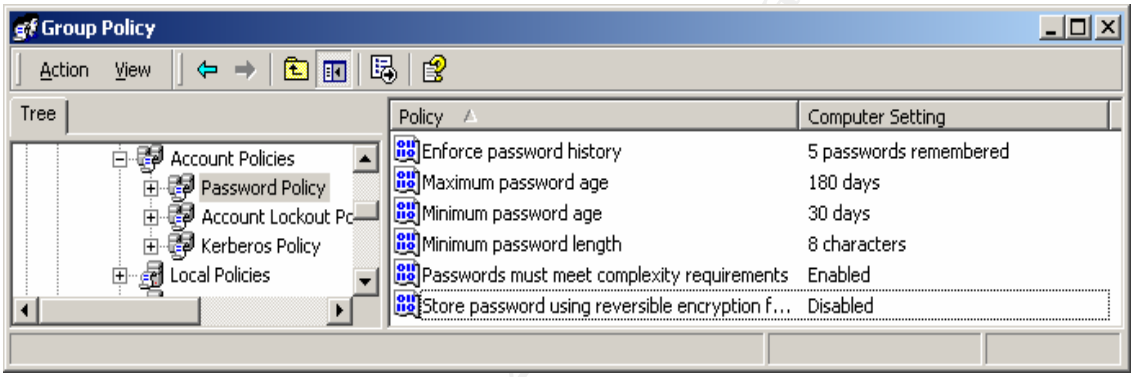
In all the following GPOs we have assigned the departments computers to a Domain Global Group which we added to the sub OU (Computers) that we created in each of the departments. Additionally we assigned the necessary Read and Apply Group Policy Access Control Entry (ACE) to each OU as needed. The Enterprise Admins, Domain Admins, and Tier III support personnel have been assigned Full Control of these GPOs.

Default Domain Policy

Our Default Domain Policy settings will be minimum Computer Configuration settings for all Domain users unless they are covered by one of our more restrictive OUs. As discussed previously, we have disabled the User Configuration portion of the domain policy to speed the application of the computer configuration settings. The application of the Computer Configuration happens prior the user even logging into the domain. This policy will be applied to the Computers OU within the following parent OUs: Executive Group OU, Sales and Marketing OU and the IT Group OU. The Resource and Development, Finance and Human Resources and the resources sub OU within the IT Group will have their own more secure GPOs applied. We will not enable the No Override option at the site or domain levels since the same IT support groups are creating and editing all the GPOs.

In selecting our password policies we wanted to require the best security that we could realistically expect the users to accept. If we made the password requirements too easy, our passwords could be simply guessed, discovered through social engineering or broken by widely available tools such as L0phtCrack. Had we been exceptionally strict in our requirements users would resist our efforts at improved security by: writing down and storing their passwords next to their systems or overwhelming our IT support staff with requests to unlock user accounts or reset passwords.

The first settings we will modify will be the Password Policy:



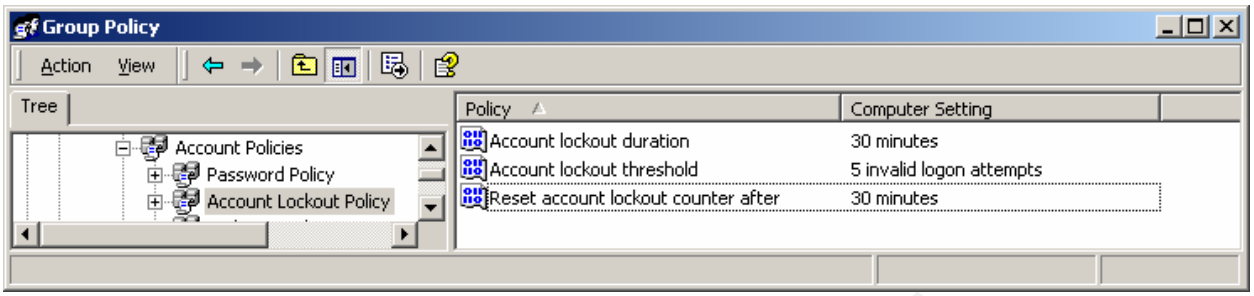
- Enforce password history: 5 passwords remembered & Minimum password age: 30 days
  - Ensures users do not reuse the same password or try and rapidly change their password in a short period of time to allow them to continue using their original password

- Maximum password age: 180
  - Ensures users change their passwords at least twice a year

- Passwords must meet complexity requirements: Enabled
  - Forces users to choose strong passwords that contain neither some or all of their username and they must additionally contain three of the four following items: upper case characters A-Z, lower case characters A-Z, a number 0-9, or a special character (e.g., !, $, #, %)

- Store password using reversible encryption for all users in the domain: Disable
  - does not allow passwords to be stored or retrieved in clear text. As this is a pure Windows 2000 network there is no reason to enable this setting.

The next setting for our Domain Group Policy will be the Account Lockout Settings:



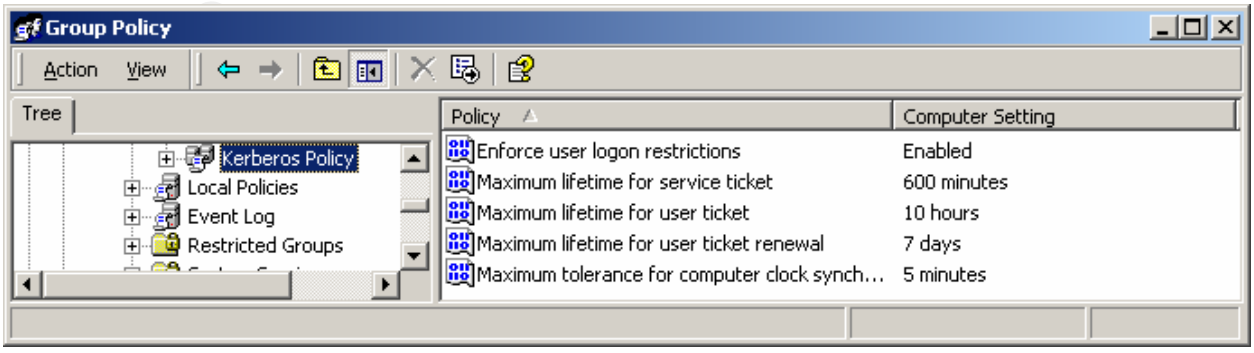
- Account lockout duration: 30 minutes
  - 30 minutes will long enough to stop crackers from trying brute force passwords cracking attacks, but not unreasonably long for users to wait if they happen to lock themselves out of their account

- Account lockout threshold: 5 invalid logon attempts
  - This gives users a little flexibility if they mistype their username or password. Usually they will notice if the cap locks was inadvertently left within 5 tries

- Reset account lockout counter after: 30 minutes
  - 30 minutes will long enough to stop crackers from trying brute force passwords cracking attacks, and will also prevent users from accumulating 5 invalid logon attempts over time and locking themselves out of their account

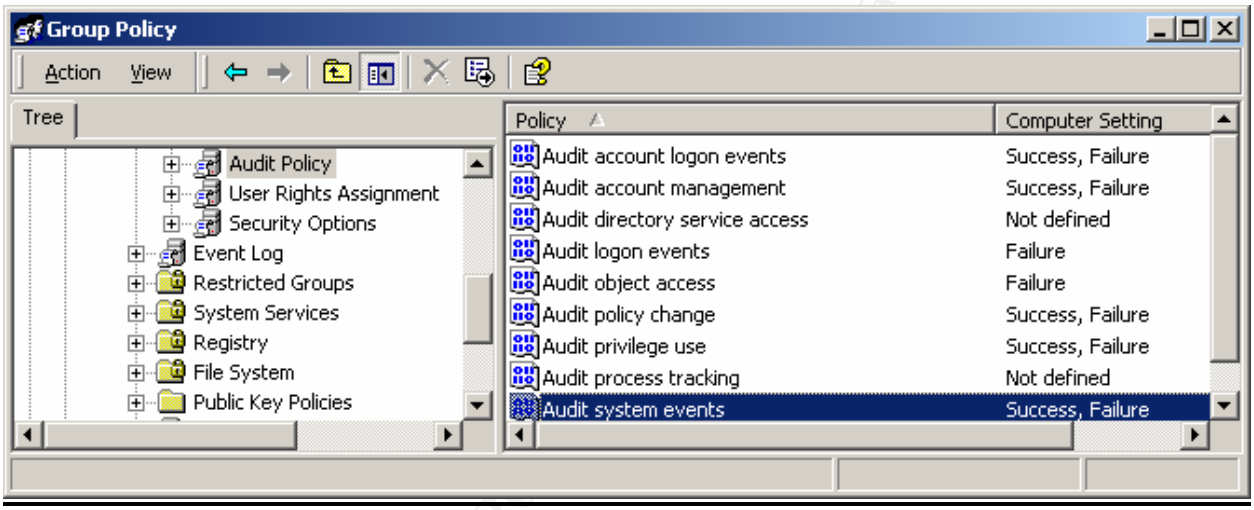
In a Windows 2000 network the domain maintains a Key Distribution Center (KDC) whose job it is to validate every request for a session ticket by examining the user rights policy on the target computer to verify that the user has the right to log on locally or access the computer across the network. The KDC also checks to ensure the account issuing the request is still valid in the domain. Administrators must choose to require the additional verification step because it may slow network access to services. The default setting is Enabled.

The next setting we will mandate for all computers will be the Kerberos Policy:



These are the default settings. Kerberos authentication is enabled, service ticket, user ticket and user ticket renewal settings are all configured to ensure the granted access remains valid over a reasonable amount of time. As the duration of these settings is increased it also increases the risk of a user gaining unauthorized access. If the duration is too short it will cause unnecessary network traffic without an effective increase in the resulting security of the network resources.

Another important area we are going to require is the Audit Policy settings:



- Audit account logon events: Success, Failure
  - maintains a record of all network logons

- Audit account management: Success, Failure
  - records creation, modification, or deletion of users and groups and password changes

- Audit directory service access: Not defined (default setting)
  - this setting records access to the Active Directory, it is only enabled on Domain Controllers

- Audit logon events: Failure
  - records local or network logon failures on the local machine

- Audit object access: Failure
  - this setting will audit failed object access

- Audit policy change: Success, Failure

- setting will audit security policy changes, including privilege assignments, audit policy modifications, and trust modifications. These settings are especially important to audit as these settings should be changed quite infrequently and only by higher level administrators.

- Audit privilege use: Failure
  - tracks when a user tries to exercise a predefined user right for which they do not have the necessary permissions

- Audit process tracking: Not defined (default setting)
  - tracking of process invocation, duplicate process handles, indirect object access, and process termination

- Audit system events: Success, Failure
  - this tracks events the effect the security log e.g., system shutdowns and restarts. These are important to track as many Trojan programs require a reboot of the system to activate

The next Domain Policy we will examine is the User Rights assignment. We have chosen to make very few modifications here as the majority of these setting that require additional security will be made in our other three OUs. The settings we will enforce with the Domain GPO include:

- Access this computer from the network: Administrators, Authenticated Users
  - there should be no reason for remote anonymous or guest access

- Back up files and directories: Enterprise Admins, IT Support, and Domain Admins
  - as we have implemented mapped home directories on the file server for each users and perform daily backups of the file server, there is no reason users should perform local backups

- Create permanent shared objects: Enterprise Admins, IT Support, and Domain Admins
  - we do not allow users to create local shares as we have a central file server that is managed by our IT department. Local shares frequently have little to no security protecting them and can be very lucrative targets to outsiders or even disgruntled employees.

- Manage auditing and security log: Enterprise Admins, IT Support, and Domain Admins
  - These logs can provide evidence of unauthorized usage or access and as such must be protected from casual modification

- Shut down the system: Enterprise Admins, IT Support, and Domain Admins

- We plan to schedule remote software installation/upgrades, Anti-virus definition updates and network vulnerability scans. The IT Group needs the systems to remain powered on by default, to provide this type of network administration support.

The next Domain Policy we will enforce is the Security Options. As with the Users Rights we will make only the minimum changes here and rely on the stricter settings on our Research and Development, Finance and Human Resources and the resources sub OU in the IT Group OU to provide additional security.

- Allow system to be shut down without having to logon: disabled
  - this ensures only authorized users are able to shutdown or restart machines by forcing them to first log on successful before shutting down

- Digitally sign client communications (always): enabled
  - Windows 2000 Professional supports Server Message Block (SMB) mutual authentication, it prevents a "man-in-the-middle" attack and also supports message authentication, which prevents active message attacks. For this authentication to work it must be at least enabled on both the server and the client. In our domain we always digitally sign client and server communications. Although the system performing the signing does experience an additional CPU load we feel it will not be significant to our network as we are using entirely new clients and servers.

- Do not display last user name in logon screen: enabled
  - in the default configuration, the user name of the last user to log on is displayed in the username field during log on. We have chosen to enable this function to hide the last logged on user name as it will be a little more difficult to gain authorized entry if one has to guess the username and password and not just the password.\

- LAN Manager Authentication Level: send NTLMv2 response only \refuse LM & NTLM
  - we have chosen to require NTLMv2 authentication since all clients are running Windows 2000. NTLM is used for pre-SP4 NT 4.0 systems and LM authentication is used by Windows 95 and 98 systems.

- Message text for users attempting to logon: You are entering a computer system of the LuckyBoyFortune Corporation. Do not try to enter unless you have a valid domain username and password. Don't try something you will later regret!

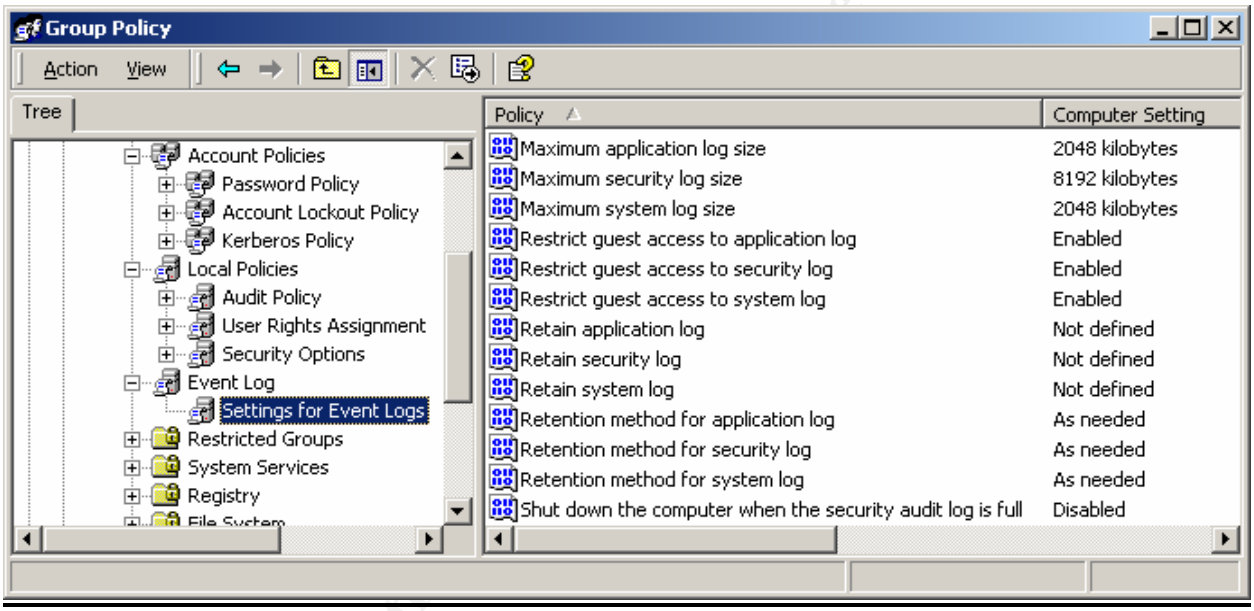
- Message title for users attempting to logon: STOP AND THINK

- Number of previous logons to cache (in case domain controller is not available):5
  - this setting can ensure users receive their normal domain desktop settings even if the DC is unavailable

- Rename administrator account: change to something other than administrator
  - renaming the default local administrator account is one of the simplest and most overlooked ways to increase the security on a network.

- Rename guest account: change to something other than guest
  - renaming the default local guest account is another overlooked and simple way to increase the security on a network. Even though this account is disabled by default, it is still a good idea to ensure it is renamed and a password is set in case it is ever re-enabled.

The last settings we will mandate for the Computer Configurations of the Executive Group OU, Sales and Marketing OU and the IT Group OU are Event Log settings



- Maximum application log size, Maximum security log size, Maximum system log size: Increase from the default size of 512KB
  - it is important to increase the log sizes to ensure an accurate and useful log of events is maintained to be used in troubleshooting or investigating potential system compromises. As an added measure of security it is a good idea to archive the security logs to a file server. It is also possible to purchase 3rd party applications that can provide automated event log analysis.

- Restrict guest access to application log, Restrict guest access to security log, Restrict guest access to system log: All these setting ensure only authorized users are allowed to view or modify the potentially sensitive information in these logs.

- Retain allocation log, Retain security log, Retain system log: Not defined

- Retention method for application log, Retention method for security log, Retention method for system log: All logs will be over written as needed, based on the 2048, 8196 and 2046KB limits previously established.

- Shut down the computer when the computer security event log is full: disabled

Default Domain Controller Policy

Many of the Default Domain Controller GPO settings are the same as those configured in our Default Domain Policy. Some additional restrictions and security measures have been added. The Default Domain Controller Policy will apply to our single LuckyBoyFortune.com place holder domain controller as well as our two Corp.LuckyBoyFortune.com domain controllers. As these settings are designed to apply to only the Computer Configuration Settings and not the user settings we will check the box disabling the User Configuration Settings on this GPO. The following settings have been changed from the Domain Policy previously created:

Account Settings > Password Policy

- Maximum password age: 90 days
  - Ensures administrators change their passwords at least quarterly

Local Policies > Audit Policy

- Audit directory service access: Failure
  - this setting records a users failure to access the Active Directory, this setting is only enabled on Domain Controllers

Local Policies > User Rights Assignment

- Access this computer from the network: Administrators, Authenticated Users
  - there should be no reason for remote anonymous or guest access

- Back up files and directories: Enterprise Admins, and Domain Admins
  - the DCs are included in the scheduled back up rotation we have for all the servers in the domain

- Create permanent shared objects: Enterprise Admins, and Domain Admins
  - There should be no local shares created on the DCs

- Log on locally: Enterprise Admins, and Domain Admins
  - there is no reason that normal domain users should be allowed to log on locally to the DCs

- Manage auditing and security log: Enterprise Admins, and Domain Admins
  - These logs can provide evidence of unauthorized usage or access and as such must be protected from casual modification. This setting is extremely important on the DCs as they hold the AD database and are potentially a very alluring target to unauthorized users

- Shut down the system: Enterprise Admins, and Domain Admins
  - DCs will only be rebooted when absolutely necessary. Situations where a reboot could be required include: addition of a new Windows 2000 Service Pack, Hotfix or other critical application. If DCs have to be rebooted we will stagger the reboots to ensure at least one is always possible to service the domain clients.

Local Policies > Security Options

- Rename administrator account: change to something other than administrator
  - change to something unique to only the Domain Controllers. Renaming the default local administrator account is one of the simplest and most overlooked ways to increase the security on a network. As an added level of protection each of our four GPOs will each use a unique name for the administrator account.

- Rename guest account: change to something other than guest
  - change to something unique to only the Domain Controllers. Renaming the default local guest account is another overlooked and simple way to increase the security on a network. Even though this account is disabled by default, it is still a good idea to ensure it is renamed and a password is set in case it is ever re-enabled. As an added level of protection each of our four GPOs will each use a unique name for the guest account.

- Digitally encrypt or sign secure channel data (always): Enabled
  - All our domain controllers are running Windows 2000 Server so they are capable of signing or encrypting all secure channel data

- Digitally encrypt secure channel data (when possible): Enabled (default setting)
  - requires all secure channel traffic be encrypted if the partner domain controller is also capable of encrypting all secure channel traffic

- Digitally sign secure channel data (when possible): Enabled (default setting)
  - requires that all secure channel traffic be signed if the partner domain controller is also capable of signing all secure channel traffic

- Shut down immediately if unable to log security audits: Enabled
  - on all servers we have implemented a plan to archive and clear the security logs weekly. If the security log which is set over 8MB fills up and shuts down the DC something is very wrong and it needs immediate attention.

Research and Development OU

With the widespread adoption of the internet in recent years it has become tougher and tougher to create and protect our fortune cookie fortunes prior to their public releases. The R&D OU has been designed to apply a greater degree of security than we mandated to the computer systems in the Executive Group, Sales & Marketing, or the IT Group. We have configured a more secure GPO due to the sensitivity of the data processed and the absolute need for secrecy in maintaining this corporate knowledge. The following settings are applied above the settings previously identified in the domain policy GPO.

Local Policies > User Rights Assignment

- Access this computer from the network: Administrators, R&D Users Group
  - there should be no reason for remote anonymous or guest access

- Back up files and directories: Enterprise Admins, and Domain Admins
  - the fortunes are maintained on a hidden file share which are included in the scheduled back up rotation we have for all the servers in the domain. The fortune shares and strictly protected with NTFS ACL which have been configured through the R&D GPO > Computers > Properties > GPO > Computer Configuration > Windows Settings > Security Settings > File System

- Create permanent shared objects: Enterprise Admins, and Domain Admins
  - There should be no local shares created on any of the sensitive systems within the R&D department

- Manage auditing and security log: Enterprise Admins, and Domain Admins
  - These logs can provide evidence of unauthorized usage or access and as such must be protected from casual modification. This setting is extremely important on the sensitive R&D systems as they are potentially a very valuable target to competition

Local Policies > Security Options

- Rename administrator account: change to something other than administrator
  - change to something unique to only the Research & Development department. Renaming the default local administrator account is one of the simplest and most overlooked ways to increase the security on a network.

- Rename guest account: change to something other than guest
  - change to something unique to only the Research & Development department. Renaming the default local guest account is another overlooked and simple way to increase the security on a network. Even though this account is disabled by default, it is still a good idea to ensure it is renamed and a password is set in case it is ever re-enabled.

- Digitally encrypt or sign secure channel data (always): Enabled
  - All our domain controllers are running Windows 2000 Server so they are capable of signing or encrypting all secure channel data

- Digitally encrypt secure channel data (when possible): Enabled (default setting)
  - requires all secure channel traffic be encrypted if the partner domain controller is also capable of encrypting all secure channel traffic

- Digitally sign secure channel data (when possible): Enabled (default setting)
  - requires that all secure channel traffic be signed if the partner domain controller is also capable of signing all secure channel traffic

- Shut down immediately if unable to log security audits: Enabled
  - on all servers we have implemented a plan to archive and clear the security logs weekly. If the security log which is set over 8MB fills up, and shuts down the R&D systems, then something is very wrong and it needs immediate attention.

Finance and Human Resources OU

Much of the financial data and Human Resources records contain information that is valuable to both our competitors and our own employees. Imagine a competitor seeing where we buy our fortunes our seeing the health officials we have to bribe to keep our factory open. Imagine an employee who finds out he is making $ 20,000 less a year than the guy with the identical position at the cubicle next door! The Finance and Human Resources OU has been designed to apply a greater degree of security than we mandated to the computer systems in the Executive Group, Sales & Marketing, or the IT Group. We have configured a more secure GPO due to the sensitivity of the data processed and the absolute need for secrecy in maintaining this corporate knowledge. The following settings are applied above the settings previously identified in the domain policy GPO.

Local Policies > User Rights Assignment

- Access this computer from the network: Administrators, F & HR Users Group
  - there should be no reason for remote anonymous or guest access

- Back up files and directories: Enterprise Admins, and Domain Admins
  - the personnel records are maintained on a hidden file share which are included in the scheduled back up rotation we have for all the servers in the domain. This share is also strictly protected with NTFS ACL which have been configured through the Finance and Human Resources GPO > Computers > Properties > GPO > Computer Configuration > Windows Settings > Security Settings > File System

- Create permanent shared objects: Enterprise Admins, and Domain Admins
  - There should be no local shares created on any of the sensitive systems within the Finance and Human Resources department

- Manage auditing and security log: Enterprise Admins, and Domain Admins
  - These logs can provide evidence of unauthorized usage or access and as such must be protected from casual modification. This setting is extremely important on the sensitive Finance and Human Resources systems as they are potentially a very valuable target to competition or our own employees

Local Policies > Security Options

- Rename administrator account: change to something other than administrator
  - change to something unique to only the Finance and Human Resources department. Renaming the default local administrator account is one of the simplest and most overlooked ways to increase the security on a network.

- Rename guest account: change to something other than guest
  - change to something unique to only the Finance and Human Resources department. Renaming the default local guest account is another overlooked and simple way to increase the security on a network. Even though this account is disabled by default, it is still a good idea to ensure it is renamed and a password is set in case it is ever re-enabled.

- Digitally encrypt or sign secure channel data (always): Enabled
  - All our domain controllers are running Windows 2000 Server so they are capable of signing or encrypting all secure channel data

- Digitally encrypt secure channel data (when possible): Enabled (default setting)
  - requires all secure channel traffic be encrypted if the partner domain controller is also capable of encrypting all secure channel traffic

- Digitally sign secure channel data (when possible): Enabled (default setting)
  - requires that all secure channel traffic be signed if the partner domain controller is also capable of signing all secure channel traffic

- Shut down immediately if unable to log security audits: Enabled
  - on all servers we have implemented a plan to archive and clear the security logs weekly. If the security log which is set over 8MB fills up, and shuts down the Finance and Human Resources systems, then something is very wrong and it needs immediate attention.

Resources sub OU

We decided to create a separate OU to hold our File Server, Microsoft Exchange 2000 Server and our External DNS Server as these three servers are critical to our IT infrastructure. Although we have decided to initially include our Exchange Server and External DNS Server, located in the screened subnet, in our domain we are diligent in reviewing the IDS and Firewall logs to ensure they are not overly vulnerable to exploit due to their domain membership. Many of these setting mimic the Default Domain Controller settings:

Account Settings > Password Policy

- Maximum password age: 90 days
  - Ensures administrators change their passwords at least quarterly

Local Policies > User Rights Assignment

- Access this computer from the network: Administrators, Authenticated Users
  - there should be no reason for remote anonymous or guest access

- Back up files and directories: Enterprise Admins, and Domain Admins
  - these servers are included in the scheduled back up rotation we have for all the servers in the domain

- Create permanent shared objects: Enterprise Admins, and Domain Admins
  - There should be no local shares created by normal users on the servers

- Log on locally: Enterprise Admins, and Domain Admins
  - there is no reason that normal domain users should be allowed to log on locally to these servers

- Manage auditing and security log: Enterprise Admins, and Domain Admins
  - These logs can provide evidence of unauthorized usage or access and as such must be protected from casual modification. These servers all make lucrative targets so the administrators must continuously review these logs

- Shut down the system: Enterprise Admins, and Domain Admins
  - servers will only be rebooted when absolutely necessary. Situations where a reboot could be required include: addition of a new Windows 2000 Service Pack, Hotfix or other critical application.

Local Policies > Security Options

- Rename administrator account: Not defined

- change to something unique to only that individual server. Renaming the default local administrator account is one of the simplest and most overlooked ways to increase the security on a network.

- Rename guest account: Not defined
  - change to something unique to only that individual server. Renaming the default local guest account is another overlooked and simple way to increase the security on a network. Even though this account is disabled by default, it is still a good idea to ensure it is renamed and a password is set in case it is ever re-enabled.

- Digitally encrypt or sign secure channel data (always): Enabled
  - All our domain controllers are running Windows 2000 Server so they are capable of signing or encrypting all secure channel data

- Digitally encrypt secure channel data (when possible): Enabled (default setting)
  - requires all secure channel traffic be encrypted if the partner domain controller is also capable of encrypting all secure channel traffic

- Digitally sign secure channel data (when possible): Enabled (default setting)
  - requires that all secure channel traffic be signed if the partner domain controller is also capable of signing all secure channel traffic

- Shut down immediately if unable to log security audits: Enabled
  - on all servers we have implemented a plan to archive and clear the security logs weekly. If the security log which is set over 8MB fills up and shuts down the server something is very wrong and it needs immediate attention.

This concludes our current level of Group Policy Object. Although we have focused on the Computer Configurations Settings up to this point we are planning so modifications affecting the User Configurations in the near future. Some of the items we plan to implement include:

- Creating software installation packages (msi.) to assign mandatory software to all systems: Windows Service Packs and hotfixes

- Creating software installation packages (msi.) to assign specific applications to individual OUs: Microsoft Publisher to the Sales and Marketing OU

- Using folder redirection to control the default path where users will save their data

To continue to ensure our Group Policy applications are working as advertised we will use two tools provided by Microsoft.The first tool: GPResult (included in Windows 2000 Server) is a command line tool that displays the resulting GPO on a computer or user. The second tool: Fazam 2000 Reduced Functionality Version (included in the Windows 2000 Server Resource Kit) features a resultant set of policies

feature, displays the history of the GPOs applied, performs a GPO search and can perform a GPO backup and restore.

The additional security settings for our domain which are not possible to deploy with a GPO would focus on our web server: LuckyBoyFortune.com
The most obvious configuration changes would include:

- Start with a fresh load of Windows 2000 Server and IIS 5.0. Do not load any unnecessary applications.

- Configure web server with the most recent Service Packs and Hotfixes, as directed by the Microsoft Technet Security Website:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp?productid=16&servicepackid=7

- Ensure to apply the MS01-044 Cumulative Patch from August 15, 2001

- Configure and maintain the web server using the Microsoft Secure Internet Information Services 5 Checklist:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/iis5chk.asp

The above detailed Secure Network Infrastructure has been running for 2 months now. We have had to modify and even re-modify certain objects and rights but so far we are very pleased with the security of this design. We have seen a significant reduction in our administrative work load since implementing a pure Windows 2000 Domain. It has been especially nice to be able to further delegate many of the more repetitive tasks, such as adding workstations to the domain or resetting passwords to the departmental Tier I and Tier II IT Support personnel.

As our comfort level with Active Directory and Group Policy increases we, like all good IT folks, are beginning to day dream of even more secure and of course complex additions to our network. Our Marketing and Research and Development Group Managers have recently mentioned sending their staffs out to our customer restaurant locations to secretly observe customers reactions when they open a LuckyBoyFortune after finishing their meal. Once back at their hotels after a long and incredibly filling day sleuthing around the local Chinese restaurants they would need to connect to our corporate LAN to report their findings. To ensure absolute secrecy of this highly sensitive market research, we are investigating setting up Virtual Private Network (VPN) into our VelociRaptor Firewall. As an added layer of security there has been talk of standing up our own Enterprise Certificate Authority (CA) to issue certificates for the traveling personnel.

Conclusion

Ultimately the security of LuckyBoyFortune's network and all networks rely on a layered approach for the most effective security. We must employ a model in which the users are educated, proper policy is in place and enforced, the physical surroundings are secured, and the hardware and software we choose to run is religiously patched and maintained. Network security is an ongoing effort that has both procedural and physical commitments. Microsoft has made exceptional progress in the security realm recently, and Windows 2000 Active Directory and Group Policy are proving themselves as very effective tools in helping us all automate our network security configuration management.

REFERENCES

1. Symantec Corporation, Enterprise Security, Symantec VelociRaptor™ 1.1, URL:

http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=49&PID=9025613
(8 Nov. 2001).

2. Microsoft Corporation, Security Bulletin Search, Windows 2000 Advanced Server with Service Pack 2,
URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp?productid=7&servicepackid=2 (9 Nov. 2001)

3. Microsoft Corporation, Security Bulletin Search, Start Page,
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp?productid=16&servicepackid=7 (9 Nov. 2001)

4. Fossen, Jason. Windows 2000: Active Directory and Group Policy, SANS Institute, 1 Jun. 2001. Pg 111-112.