1

Information Systems Audit & Control Association

Windows 2000/Active Directory Security

Presented by: Deloitte & Touche Raj Mehta – CPA, CITP, CISA, CISSP Denis Tiouttchev – CIA, CISA, CISSP

August 21, 2003



Focus

- Introduction to Windows 2000 and Active Directory
- Organizational Unit (OU) Concept
- Group Policy Objects (GPOs)
- Windows 2000 Groups
- File System
- File Permissions / Access Control Lists
- Registry Permissions
- Security Templates
- Rights
- Demo
- Audit Checklist



Introduction to Windows 2000

Windows 2000 is essentially Windows NT 5.0

Contains many new security features

- Active Directory
- Kerberos Authentication Protocol
- Encrypting File System
- IPSec, PKI, & Smartcards

NT versus Win2K (AD)

NT	Windows 2000
PDC & BDC	Domain Controllers w/Active Directory
NTLM Authentication (Weaker Form)	Kerberos (Stronger Authentication)
No native file encryption utility	Encrypting File System (EFS)
РРТР	IPSec
N/A	PKI, Smartcards
File System (Share & NTFS Permissions)	Same
Trusts Among Domains need to be defined	Automatic two-way trust between Win2K domains and Forests
System Policies	Centralized configuration through GPOs
N/A	Custom Permissions and Delegation of Authority
Syskey not automatically enabled	Syskey automatically enabled

Introduction to Active Directory

Active Directory (AD) is Windows 2000's directory service and is accessed through Lightweight Directory Access Protocol (LDAP).

AD is the core policy & configuration repository for each component of Windows 2000 providing most importantly:

- Centralized security configuration of all computers in the domain via Group Policy Objects
 - Local account, lockout and audit policy
 - Services
 - ◆ File, Registry, & Printer Permissions
 - User Rights
 - Event Log Settings

What does AD provide?

- Single Sign-on User Database
 - Windows 2000
 - Exchange & Lotus Notes
 - ♦ SQL Server
 - ERP (SAP, Oracle, PeopleSoft)
- Granular delegation of administrative authority
- Centralized security configuration of all users and computers in the domain.
 - Local Account, lockout and audit policy
 - Services
 - Registry Permissions
 - Printer Permissions
 - ♦ User Rights
 - Event Log settings

AD Concepts

Computers, users, groups, printers, shared file server directories, etc. are organized and controlled according to the enterprise's organizational hierarchy, which are represented through a number of container objects:

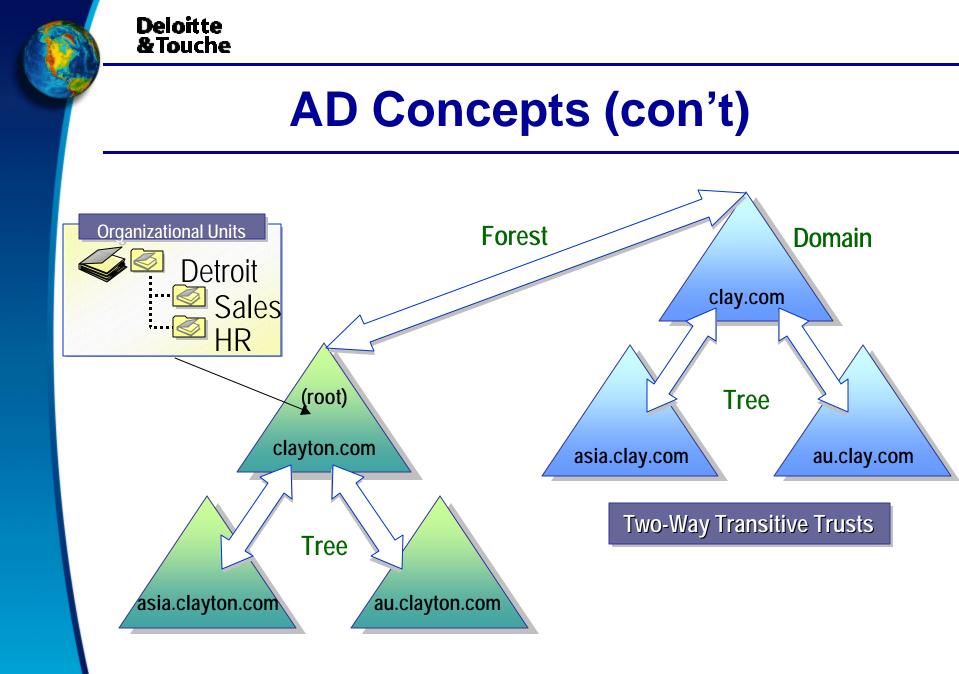
- Domains fundamental container in Active Directory that can hold all of the users, computers, etc for an entire organization
- Organizational Units (OU) used to subdivide objects within a domain that typically correspond to a division, department, region, etc.
- Trees used in multiple domain environments to facilitate contiguous DNS name space & automatic trust relationships between domains
- Forests used in multiple domain environment that do not share a contiguous DNS name space
- Sites used to organize computers based on physical location to efficiently utilize network bandwidth between sites

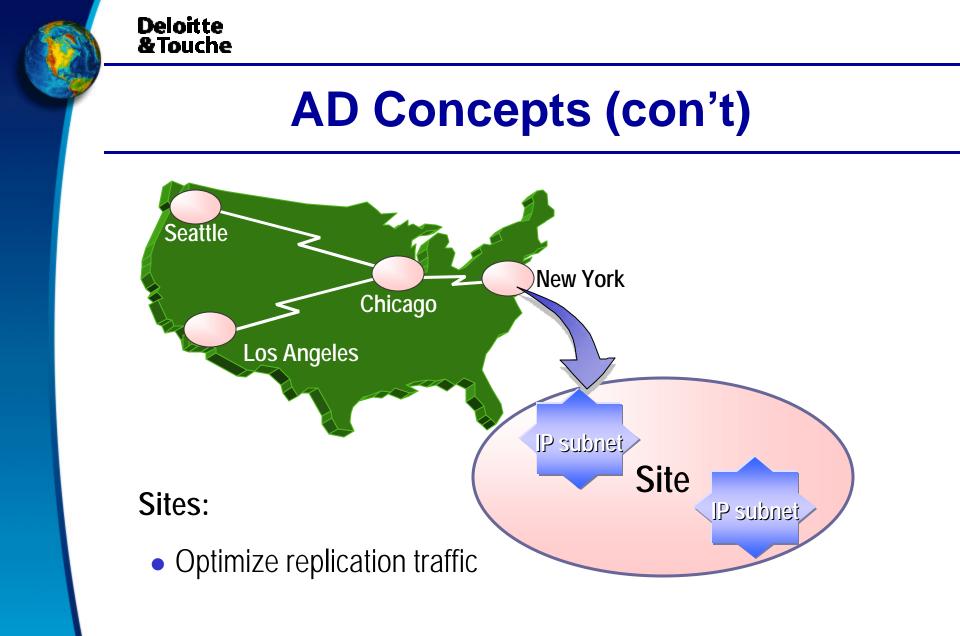
OU Considerations

How OU structure is designed is critical in terms of how the AD will be administered. It's very easy to make this a complicated process.

Factors to consider when creating OUs:

- How objects will be administered centralized versus decentralized (e.g., HR OU)
- What type of GPOs will be enforced: User Level (General Users versus Special Users); Machines (Workstation versus Servers)
- How information needs to be organized





Group Policy Objects

Group Policy Object (GPO) - the avenue for central security configuration within Windows 2000 and Active Directory

- GPOs provide a way to manage all of the configuration changes and policy settings utilizing the hierarchy of Active Directory
- GPOs can be applied to Users and Computers within an OU (e.g. map drives, screen savers, etc.), but can not be applied to Groups within an OU

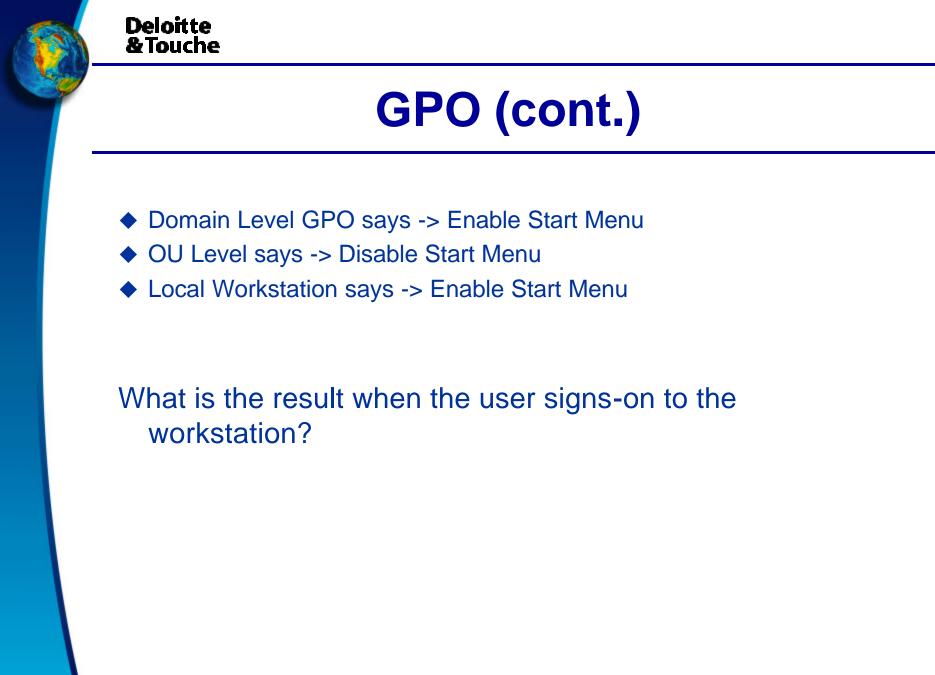
- GPO Application Order: L(Local). S(Site). D (Domain).
 OU(Organizational Unit)
- If multiple conflicting GPOs within same level, last GPO wins!
- You can block inheritance from top level GPOs
- GPO can be defined or undefined

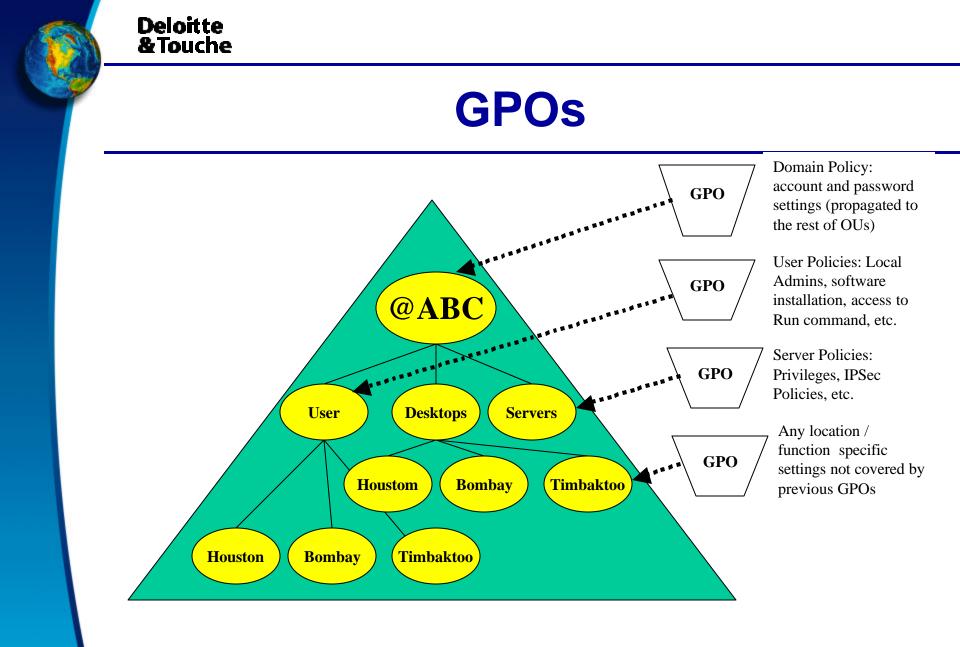
Group Policy Objects (cont.)

• Example of Computer Configurations:

 Account Policies (Password & Account Lockout Policy) – Defined only Once at Domain Level)

- Audit Policy
- User Rights Assignment
- Security Options (e.g., do not display last user name in logon screen)
- Setting for Event Logs
- Example of User Configurations:
 - Remove Control Panel Access
 - Remove Run command Access
 - Internet Explorer Options
 - Screen Saver Options







Key Groups

Prior to delegation, check memberships to the following built-in groups:

Member Server/Workstation – Administrator

 Domain Level – Administrators, Domain Admins, Account Operators, Server Operators, Backup Operators, Print Operators, DNSAdmins

1

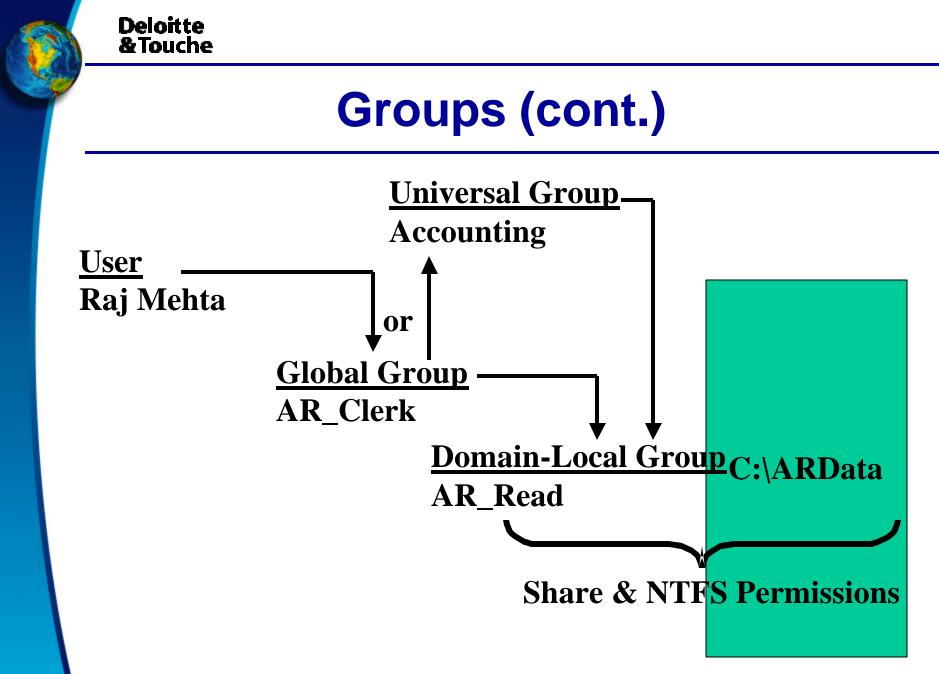
Each Forest – Enterprise Admins, Schema Admins

Groups (cont.)

Group Types: Security versus Distribution Groups

Group Categories for Security Groups:

Group	Can Contain	Permissions Granted
Universal (Defined at AD)	Users, Global Groups, Universal Groups (any domain in the forest)	Anywhere in the forest
Global (Defined at AD)	Users, other Global Groups (from same domain)	Anywhere in the forest
Domain Local (Defined at AD) – only on DC	Users, Global Groups, Universal Groups, and Domain Local (from same domain)	Within same domain





File System

File Systems – how info is stored on a hard drive

- NT File System (NTFS)
 - Security attributes that can be applied to a file or folder via ACLs
 - Higher performance
 - Encryption File System
- File Allocation Table (FAT)
 - Can't use Encryption or Security
 - Very Insecure
 - DOS/WIN95 compatible
- Typically, Network Administrators have a misperception that FAT file are "Easier to Recover"
- Issue Anyone can boot to the server with a Windows 98 startup disk within the Server Driver and gain access to the SAM file



 Each printer has an ACL accessible through Control Panel/printers that controls access to the printer and the print jobs within the queue

Directory Objects

 Users, groups, and computers each have an ACL that control who can read properties of the object and perform updates

Registry Keys

- Access to the registry is managed through the Registry Editor
- Similar to folder permissions but different structure (e.g. keys, subkeys, etc.)

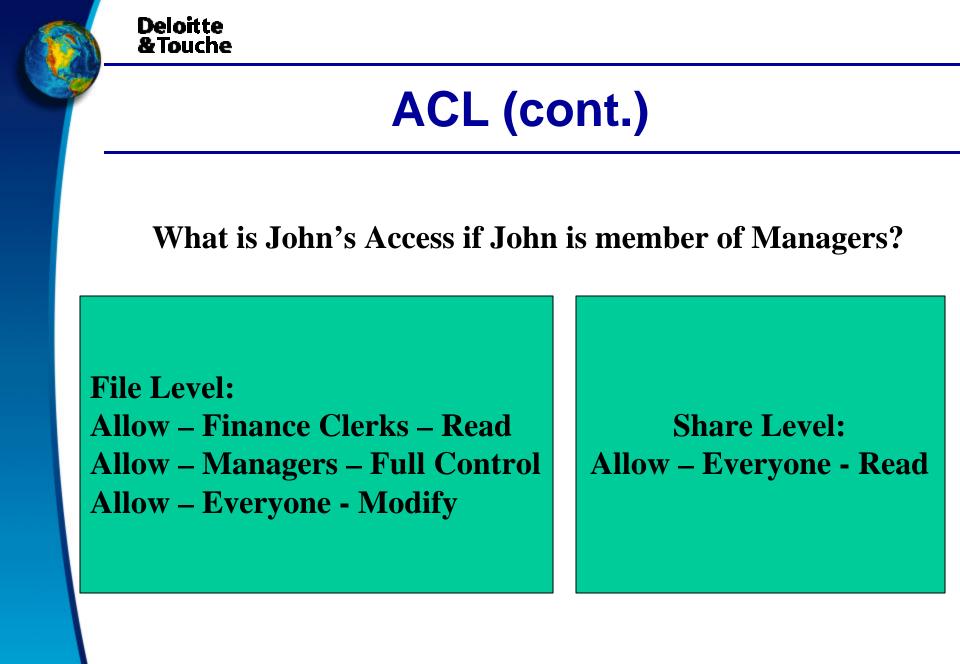


ACL (Access Control Lists)

General Rules:

- Explicit permissions overrides inherited permissions
- Deny permission always wins over Allow permissions within same category
- ACL permissions gained through group membership are cumulative
- Missing Permissions versus Blank Permissions

NTFS versus Share Permissions



Registry Permissions

- Access to Registry (security database)
 - System configuration
 - Application settings
 - User preferences and profile settings
 - Security
 - Local Users and Groups
 - Local password, lockout and audit policy
- The registry attempts to unify and give structure to all configuration data
- Contains crucial security and system related information, therefore access to the registry should be limited
- The registry is updated through:
 - Control Panel
 - Group Policies
 - Application setup programs
 - Registry Editor



Security Templates

- Security Configuration and Analysis Tool
- Security Templates:
 - C:\Winnt\security\templates
 - Basicdc.inf
 - Basicsv.inf
 - Basicwk.inf
 - Hisecdc.inf
 - Hisecwk.inf

Rights

Rights – govern who can use the system and perform specific system management functions

- Rights do not apply to specific objects
- Assigned with the "User Rights Assignment" section of the Local Policies within AD
- Medium High Risk User Rights:
 - Act as part of operating system
 - Backup files and directories
 - Restore files and directories
 - Create a token object
 - Debug programs
 - Manage auditing and security log
 - Take ownership of files or other objects
 - Enable computer and user accounts to be trusted for delegation
 - Load and unload devices
 - Shut down the system
 - Add workstations to domain
 - Access this computer from the network
 - Change the system time
 - Force shutdown from a remote system
 - Log on as a batch job
 - Log on as a service
 - Log on locally



DEMO

AUDIT CHECKLIST

Audit Checklist

- DOMAINS, FORESTS, & TRUSTS Assess the Domain & Trust structure with a focus on the appropriateness of externally (outside forest) trusted domains. Also, review the physical access of the Domain Controllers & Servers.
 - Where? Start, Programs, Administrative Tools, Active Directory Domains & Trusts, right click on the Domain, select Properties, then the Trusts tab

omain Name	Relationship	Transitive 📥	
ubsidiary19.acme.local	Child	Yes	Add
ubsidiary20.acme.local	Child	Yes	
ibsidiary21.acme.local	Child	Yes	Edit
ıbsidiary22.acme.local	Child	Yes	
ibsidiary23.acme.local	Child	Yes	Remove
ibsidiary24.acme.local	Child	Yes 🧲	
omain Name	Relationship	Transitive 🔺	
ubsidiary01.acme.local	Child	Yes	Add
ubsidiary02.acme.local	Child	Yes 🚽	
ibsidiary03.acme.local	Child	Yes	Edit
ibsidiary04.acme.local	Child	Yes	
ibsidiary05.acme.local	Child	Yes	Remove
	Child	Yes	
ubsidiary06.acme.local	Child	Va 🔟	

Audit Checklist (con't)

2) **WORKGROUPS & DOMAINS** – Verify that Domains are utilized for security and user administration.

- •
- Where? Right Click on My Computer, Properties, Network Identification tab (randomly select a few computers)

stem Properties		
General Network Iden	tification Hardware User F	Profiles Advanced
Windows us on the netwo	es the following information to ork.	o identify your computer
Full computer name:	student13.subsidiary13.a	cme.local
Domain:	subsidiary13.acme.local	
To rename this comput Properties.	er or join a domain, click	Properties
The computer is a do	n of the computer cannot be a main controller.	



3) **GROUP POLICY OBJECTS** – Obtain an understanding of the methodology for implementation of Group Policies.

 Where? – Start, Programs, Administrative Tools, Active Directory Users & Computers, Right Click select Properties then the Group Policy tab

Action View	
Period Name Period Software Settings Software Settings Software Settings Software Settings Software Settings Software Settings Software Settings Scripts (Startup/Shutdo Scripts (Startup/Shutdo Startup/Shutdo Scripts (Startup/Shutdo System Startup/Shutdo <	

Audit Checklist (con't)

4) **PERMISSIONS / ACLs** – Verify that the appropriate groups & users have been granted access to high-risk files, folders, directories, etc.

Where? – Right click on resource, properties, security tab, then select the advance tab for each entry, then click view/edit button for each entry

		Add
 £ Curly (Curly@dandt.com) Guest (SUBSIDIARY13\Guest) Minternal Auditors (SUBSIDIARY13\ 	Internal	Remove
Larry (Larry@dandt.com) Mo (Mo@dandt.com) ermissions:	Allow	Deny
Full Control		
Modify		
Read & Execute		
List Folder Contents		
Read		
Write		3 53 6

Туре	Name	Permission	Apply to	Name: Curly (Curly@dandt.com)	Lh	hange
Allow Allow Allow Allow Allow	Curly (Curly@dandt.com) Guest (SUBSIDIARY13 Internal Auditors (SUBS Larry (Larry@dandt.com) Mo (Mo@dandt.com)	Full Control Full Control Read & Exec Full Control Full Control	This folder, subfolders and files This folder, subfolders and files This folder, subfolders and files This folder, subfolders and files This folder, subfolders and files	Apply onto: This folder, subfolders an Permissions: Haverse Folder / Execute File List Folder / Read Data Read Attributes Read Extended Attributes Create Files / Write Data		
			ssion is inherited by child objects.	Create Folders / Append Data Write Attributes Write Extended Attributes Delete Subfolders and Files Delete Read Permissions Change Permissions Take Ownership		

Audit Checklist (con't)

5) **REGISTRY** – Verify which OU has access to update the Registry.

Where? – Start, Programs, Administrative Tools, Active Directory Users and Computers, right click on the selected OU select properties then Group Policy. Select the GPO, click on Edit, then review the Disable registry editing tools parameter

Policy	Setting
Group Policy Group Policy Century interpretation for Year 2000 Code signing for device drivers Custom user interface Disable the command prompt Disable registry editing tools Run only allowed Windows applications Don't run specified Windows applications	Not configure Not configure Not configure Not configure Not configure Not configure Not configure Not configure
	Policy B.st Policy Don't display welcome screen at logon Contury interpretation for Year 2000 Code signing for device drivers Custom user interface Disable the command prompt Disable registry editing tools Run only allowed Windows applications Disable Autoplay

Audit Checklist (con't)

6) FILE SYSTEMS - Verify that all disk partitions are formatted with NTFS.

Where? – Start, Programs, Administrative Tools, Computer Management

📮 Computer Management								_ 8 >
Action View	2 5							
Tree	Volume	Layout	Туре	File System	Status	Capacity	Free Space	% Free
Computer Management (Local) System Tools System Tools System Information System Information Shared Folders Device Manager Local Users and Groups	(C:)	Partition Partition	Basic Basic	FAT NTFS	Healthy (System) Healthy (Boot)	995 MB 1.95 GB	989 MB 441 MB	99 % 22 %
E Storage	•							P
	Disk 0 Basic 28.62 GB Online	(C:) 996 MB FAT Healthy (System)		(D:) 1.95 GB NTFS Healthy (Boot)		25.69 GB Free Space		
	CDRom 0 CDRom (E:)							
	Princer Patilitie	n 🗖 Extended Partit		Logical Drive				

33



7) **SERVICE PACK / SYSTEM PROPERTIES**- Verify the Windows 2000 system properties and service pack installed

 Where? – Start, Run, type "MSINFO32" or right click on My Computer and select Properties

Tree	Item	Value	
Jystem Information	OS Name	Microsoft Windows 2000 Server	
	Version	5.0.2195 Build 2195	
🗄 🚞 Hardware Resources	OS Manufacturer	Microsoft Corporation	in the second
🗄 🦲 Components	System Name	STUDENT13	
🗄 🧰 Software Environment	System Manufacturer	D815EA	
🗄 🧰 Internet Explorer 5	System Model	EA81510A	
	System Type	X86-based PC	
	Processor	x86 Family 6 Model 8 Stepping 3 GenuineIntel ~731	
	BIOS Version	06/28/00	
	Windows Directory	D:\WINNT	
	Locale	United States	
	Time Zone	Central Daylight Time	
	Total Physical Memory	522,544 KB	
	Available Physical Memory	394,928 KB	
	Total Virtual Memory	1,799,524 KB	
	Available Virtual Memory	1,546,168 KB	
	Page File Space	1,276,980 KB	

em Properties	<u>? × </u>
neral Network Identification Hardwa	are User Profiles Advanced
Sj	vstem:
	Microsoft Windows 2000
	5.00.2195
B	egistered to:
	·
	51876-270-4551042-05757
Ci	omputer:
	x86 Family 6 Model 8 Stepping 3
	AT/AT COMPATIBLE
	522,544 KB RAM
OK	Cancel Apply
- OK	

Audit Checklist (con't)

8) **PROTOCOLS** - Verify the network/system protocols installed.

Where? – Right click on My Network Places, select Properties, Right click on the applicable Connections, select Properties

	n 2 Properties	
neral Sharing		
onnect using:		
Intel(R) PRO/1	00 VE Network Connection	
		Configure
omponents checked	are used by this connection	: :
🛛 🔜 Client for Micro	osoft Networks	
	er Sharing for Microsoft Netw	orks
🖊 🏺 Internet Proto		
🖞 🏺 Internet Proto		
🖞 🏺 Internet Proto		
Install	Uninstall	Properties
Install		Properties
Description		
Install Description Allows your comput	Uninstall	
Install Description Allows your comput network.	Uninstall	
Install Description Allows your comput network.	Uninstall	
Install Description Allows your comput network.	Uninstall	

Audit Checklist (con't)

9) **SERVICES** - Examine what services are enabled and ensure that unnecessary and potentially insecure services are disabled (e.g. ftp, telnet, smtp, etc.).

Where? – Start, Programs, Administrative Tools, Services

Services						_ 8			
Action View		Description Status Startup Type Log On As Notifies sel Started Automatic LocalSystem Supports C Manual LocalSystem Provides a Started Manual LocalSystem Maintains a Started Manual LocalSystem Maintains a Started Automatic LocalSystem Manages n Started Automatic LocalSystem Manages n Started Automatic LocalSystem n Manages n Started Automatic LocalSystem ng Client Sends notif Started Automatic LocalSystem							
Tree	Name A	Description	Status	Startup Type	Log On As				
Services (Local)	Alerter	Notifies sel	Started	Automatic	LocalSystem				
	Application Management	Provides s		Manual	LocalSystem				
	ClipBook	Supports C		Manual	LocalSystem				
	COM+ Event System	Provides a	Started	Manual	LocalSystem				
	Computer Browser	Maintains a	Started	Automatic	LocalSystem				
	BHCP Client	Manages n	Started	Automatic	LocalSystem				
	Distributed File System	Manages lo	Started	Automatic	LocalSystem				
	Distributed Link Tracking Client	Sends notif	Started	Automatic	LocalSystem				
	Server Distributed Link Tracking Server	Stores info	Started	Automatic	LocalSystem				
	Distributed Transaction Coordinator	Coordinate	Started	Automatic	LocalSystem				
	Southern Client	Resolves a	Started	Automatic	LocalSystem				
	Event Log	Logs event	Started	Automatic	LocalSystem				
	Fax Service	Helps you		Manual	LocalSystem				
	File Replication Service	Maintains fi	Started	Automatic	LocalSystem				
	IIS Admin Service	Allows adm	Started	Automatic	LocalSystem				
	Indexing Service			Manual	LocalSystem				
	Intel(R) Active Monitor		Started	Automatic	LocalSystem				
	Internet Connection Sharing	Provides n		Manual	LocalSystem				
	Intersite Messaging	Allows sen	Started	Automatic	LocalSystem				
	IPSEC Policy Agent	Manages I	Started	Automatic	LocalSystem				
	Kerberos Key Distribution Center	Generates	Started	Automatic	LocalSystem				
	License Logging Service		Started	Automatic	LocalSystem				
	Logical Disk Manager	Logical Disk	Started	Automatic	LocalSystem				
	Logical Disk Manager Administrative Service	Administrat	Started	Manual	LocalSystem				
	Messenger	Sends and	Started	Automatic	LocalSystem				
	Net Logon	Supports p	Started	Automatic	LocalSystem				
	NetMeeting Remote Desktop Sharing	Allows aut		Manual	LocalSystem				
	Network Connections	Manages o	Started	Manual	LocalSystem				
	Network DDE	Provides n		Manual	LocalSystem				
	Network DDE DSDM	Manages s		Manual	LocalSystem				
	NT LM Security Support Provider	Provides s		Manual	LocalSystem				
	Performance Logs and Alerts	Configures		Manual	LocalSystem				
	Plug and Play	Manages d	Started	Automatic	LocalSystem				
	Print Spooler	Loads files	Started	Automatic	LocalSystem				
	Protected Storage	Provides pr	Started	Automatic	LocalSystem				
	QoS RSVP	Provides n		Manual	LocalSystem				
	Remote Access Auto Connection Manager	Creates a		Manual	LocalSystem				
	Remote Access Connection Manager	Creates a		Manual	LocalSystem				

Audit Checklist (con't)

10) **ACCOUNTS** – Verify that the Guest account is disabled.

 Where? – Start, Programs, Administrative Tools, Active Directory Users & Computers

Active Directory Users and Co <u>Console</u> Window <u>H</u> elp				_ 8 _ 8
	🔟 🗙 🗔 😰 🙀 🌆	766		Terror Leven
ree	Users 15 objects			
Active Directory Users and Compu	Name	Туре	Description	
- Subsidiary 13. acme. local	🕵 Administrator	User	Built-in account for admini	
🗄 🧰 Builtin	Cert Publishers	Security Group - Global	Enterprise certification an	
🗄 🧰 Computers	Clayton	User		
🗄 🧭 Domain Controllers	Domain Admins	Security Group - Global	Designated administrators	
🗄 🧭 Fin	Domain Computers	Security Group - Global	All workstations and serve	
😟 🧰 ForeignSecurityPrincipals	Domain Controllers	Security Group - Global	All domain controllers in th	
🗄 🧭 Investments	M Domain Guests	Security Group - Global	All domain quests	
🖻 🧭 IT	Domain Users	Security Group - Global	All domain users	
😟 🧰 LostAndFound	Group Policy Creator Owners	Security Group - Global	Members in this group can	
🕀 🧭 Mfr	Guest	User	Built-in account for guest	
- 🙆 Mktg	IUSR_STUDENT13	User	Built-in account for anony	
	IWAM STUDENT13	User	Built-in account for Intern	
🗄 🥝 R&D		User	Key Distribution Center Se	
🕀 🧰 System	RAS and IAS Servers	Security Group - Domain Local		
Users		User	This user account is used	
>				

37

Audit Checklist (con't)

11) **ACCOUNTS** – Verify the membership of the Built-in Administrative Groups.

 Where? – Start, Programs, Administrative Tools, Active Directory Users & Computers, select the Builtin folder, double click on each Group and examine the Members tab

Active Directory Users and D	omputers			0 doo	inistrators Prop	ortios	? X
🗳 Console Window Help				18×	inistrators Prop	Eldes	
Action Yew 💠 🕈 💽		60		Ge	Members	Member Of Managed By Object Security	
Tree	Builtin 9 objects			ue	neral members	member or [managed by [object] Security [
Active Directory Users and Corpo	None	Тура	Description		lembers:		L L
E 🗊 subsidiary t 3. acrie Jocal	Account Operations	Security Group - Builtin Local	Members can administer domain user and group accounts	M	rempers:		10
Euitin	Administrators	Security Group - Builtin Local	Administrators have complete and unrestricted access to the computer/idonain		Name	Active Directory Folder	
 Computers Consum Controllers 	Badup Operators	Security Group - Builtin Local	Badiup Operators can override security restrictions for the sole purpose of bading up o	e restore			
E S Pin	Guests Pre-Windows 2000 Compatible Access	Security Group - Bultin Local Security Group - Bultin Local	Guests have the same access as numbers of the Users group by default, escapt for the A badward compatibility group which allows read access on all users and groups in the o	Guest e	💈 Administrator	subsidiary13.acme.local/Users	
E ToreignSecuritsPrincipels	Print Operators	Security Group - Bultin Local	Venbers can administer donain printiers	L(02)	🖸 Clayton	subsidiary13.acme.local/Users	
E M Investments	Replicator	Security Group - Bultin Local	Supports file replication in a domain				
E 🙆 IT	Server Operators	Security Group - Builtin Local	Wenthers can administer domain cervers			subsidiary13.acme.local/Users	
🐑 🚞 LostAndFound 🕀 🎯 Mir	Disers	Security Group - Builtin Local	Users are prevented from making accidental or intentional system-wide changes. Thus,	Users ca	Enterprise Ad.	acme.local/Users	
E B Million				1		New Contraction (New Contraction)	
E A NovAquisitions							
🗩 🎯 RAD							
(81) 🧾 System							
🖭 - 🛄 Users							
	1						
				100			-
					I	- I	
					Add	Remove	
	1						
	1						
	1					N. (8	
	1					OK Cound 1	
4						OK Cancel A	pply
<u> </u>			6 1				
				100			

38

Audit Checklist (con't)

12) **MEMBERSHIP OF GROUPS** – Obtain an understanding of the use of groups and ensure that the assignment of users to the groups is appropriate.

 Where? – Start, Programs, Administrative Tools, Active Directory Users & Computers, select the applicable groups within the OUs, double click on each Group and examine the Members tab

Active Directory Users and Co	omputers					
🧳 ⊆onsole <u>W</u> indow <u>H</u> elp				PasswordReset-Mk	tg Properties	? ×
Action View 🗍 🖛 🔿 🔁		10 10 10 10 40 10		Transa and the second		
ee	InfoSec 5 objects			Gen Console Root\A	Active Directory Users and Computers [stu	udent13.subsidiary:
Active Directory Users and Compu	Name	Туре	Descriptio			
🗊 subsidiary13.acme.local	2 PasswordReset-Fin	Security Group - Global		Members:		
🗄 🦲 Builtin	PasswordReset-IT	Security Group - Global		Name	Active Directory Folder	
	PasswordReset-Mfr PasswordReset-Mktg	Security Group - Global Security Group - Global				
	PasswordReset-R&D	Security Group - Global Security Group - Global		🖉 Jack	subsidiary13.acme.local/Mktg	
🗄 🧰 ForeignSecurityPrincipals		Jocano, arcapi alobai		🖉 Jill	subsidiary13.acme.local/Mktg	
@ Investments ⊡-@ IT				••• •••	calculate, responses and a	
Development						
🐼 InfoSec						
E Standround						
Mktg						
- 🙆 NewAquisitions						
@ R&D						
∓ 📄 System ∓ 🧰 Users						
E Users						
				10		100
				A <u>d</u> d	<u>R</u> emove	
					OK Cancel	Apply
						EPP0
	•			k	1	
	1.1					



13) **PASSWORD POLICY** – Review the appropriateness of the password parameters within the Account Policies.

Where? – Start, Programs, Administrative Tools, Active Directory Users and Computers, right click on the Domain Controllers OU select properties then Group Policy. Select the GPO, click on Edit, then review the Account Policies

gf Group Policy				_ 8 ×
Action View 🗢 🔿 🔁	• X 🖳 😰			
Tree	Policy A	Computer Setting		
Default Domain Controllers Policy [s Computer Configuration Software Settings Windows Settings Windows Settings Account Policies Count Policies Count Lockou Count Lockou	Konforce password history Maximum password age Minimum password age Minimum password length Passwords must meet complexity requirements Store password using reversible encryption f	18 passwords remembered 30 days 29 days 8 characters Enabled		
	1			
				l î



14) **ACCOUNT LOCKOUT** – Review the appropriateness of the account lockout parameters within the Account Policies.



Where? – Start, Programs, Administrative Tools, Active Directory Users and Computers, right click on the Domain Controllers OU select properties then Group Policy. Select the GPO, click on Edit, then review the Account Policies

🝠 Group Policy				_ & ×
] Action ⊻iew] 🗢 → 🔁 [
Tree	Policy A	Computer Setting		
Default Domain Controllers Policy [s	Account lockout duration	30 minutes		
Default Domain Controllers Policy [s Computer Configuration Software Settings Windows Settings Security Settings Security Settings Computer Configuration Security Settings Computer Configuration Security Settings Software Settings Softwa	Account lockout duration Account lockout threshold Reset account lockout counter after			
				1



15) **AUDIT POLICY** – Obtain an understanding of the use of auditing and ensure that the appropriate events are logged and reviewed.

 Where? –Within Group Policy select Windows Settings, Local Policies then Audit Policy. Select your object, right click properties, select security tab, advanced, select auditing tab and View/Edit

Action View Policy Policy	Object	
Tree Deline Colline Colline		
Tree Policy A Local Setting Effective Setting	1. 1. 1. Provide 1	
Security Settings Built account logon events No auditing Success, Failure Cocount Policies Built account management No auditing Success, Failure Cocount Policies Built account management No auditing Success, Failure Cocount Policies Built account management No auditing Success, Failure Cocount Policies Built addit directory service access No auditing Success, Failure Public Key Policies Budit policy change No auditing Success, Failure Budit Rey Policies Budit process tracking No auditing Success, Failure Budit process tracking No auditing Success, Failure Budit system events No auditing Success, Failure Budit system events No auditing Success, Failure	List Folder / Read Data Read Attributes Read Extended Attributes Create Files / Write Data Create Folders / Append Data Write Attributes Write Extended Attributes Delete Subfolders and Files Delete Read Permissions Change Permissions	Change

Audit Checklist (con't)

 EVENT LOGS – Inquiry as to the use of the Event Logs and frequency of reviews. Obtain a copy of the event logs.

Where? – Start, Programs, Administrative Tools, Event Viewer

e	System Log 90	event(s)							
Event Viewer (Local)	Туре	Date	Time	Source	Category	Event	User	Computer	
Application Log	🔥 Warning	4/30/2003	4:53:12 PM	Netlogon	None	5781	N/A	STUDENT13	
Security Log	Information	4/30/2003	4:34:27 PM	Removable Storage Se	None	135	N/A	STUDENT13	
📵 System Log	S Error	4/30/2003	4:33:50 PM	Removable Storage Se	None	17	N/A	STUDENT13	
Directory Service	Error	4/30/2003	4:33:35 PM	Removable Storage Se	None	17	N/A	STUDENT13	
File Replication Service	Information	4/30/2003	4:33:20 PM	Removable Storage Se	None	134	N/A	STUDENT13	
	Information	4/30/2003	4:33:20 PM	Removable Storage Se	None	135	N/A	STUDENT13	
	Information	4/30/2003	4:33:19 PM	Removable Storage Se	None	134	N/A	STUDENT13	
	Information	4/30/2003	4:25:57 PM	Application Popup	None	26	N/A	STUDENT13	
	🔥 Warning	4/30/2003	3:58:43 PM	Schannel	None	36872	N/A	STUDENT13	
	Information	4/30/2003	2:36:54 PM	Application Popup	None	26	N/A	STUDENT13	
	(Information	4/30/2003	2:25:23 PM	Application Popup	None	26	N/A	STUDENT13	
	Information	4/30/2003	2:24:20 PM	Application Popup	None	26	N/A	STUDENT13	
	(1) Information	4/30/2003	2:23:36 PM	Application Popup	None	26	N/A	STUDENT13	
	Information	4/30/2003	2:21:35 PM	Application Popup	None	26	N/A	STUDENT13	
	(Information	4/30/2003	2:06:29 PM	Application Popup	None	26	N/A	STUDENT13	
	Information	4/30/2003	11:42:12	Application Popup	None	26	N/A	STUDENT13	
	(Information	4/30/2003	11:42:08	Application Popup	None	26	N/A	STUDENT13	
	(Information	4/30/2003	11:41:38	Application Popup	None	26	N/A	STUDENT13	
	Information	4/30/2003	11:39:53	Application Popup	None	26	N/A	STUDENT13	
	(i) Information	4/30/2003	11:37:05	Application Popup	None	26	N/A	STUDENT13	
	(Information	4/30/2003	11:36:01	Application Popup	None	26	N/A	STUDENT13	
	(i) Information	4/30/2003	11:35:26	Application Popup	None	26	N/A	STUDENT13	
	(i) Information	4/30/2003	11:23:36	Application Popup	None	26	N/A	STUDENT13	
	(i) Information	4/30/2003	11:18:50	Application Popup	None	26	N/A	STUDENT13	
	(Information	4/30/2003	10:54:24	Application Popup	None	26	N/A	STUDENT13	
	(Information	4/29/2003	11:37:08	Browser	None	8015	N/A	STUDENT13	
	(i) Information	4/29/2003	11:36:52	Browser	None	8015	N/A	STUDENT13	
	Warning	4/29/2003	11:36:20	Dhep	None	1007	N/A	STUDENT13	
	Information	4/29/2003	11:35:18	eventlog	None	6005	N/A	STUDENT13	
	(i) Information	4/29/2003	11:35:18	eventlog	None	6009	N/A	STUDENT13	
	Error	4/29/2003	11:35:18	eventlog	None	6008	N/A	STUDENT13	
	Warning	4/29/2003	11:35:29	disk	None	34	N/A	STUDENT13	
	Warning	4/29/2003	8:59:29 AM	Schannel	None	36872	N/A	STUDENT13	
	Warning	4/29/2003	1:54:21 AM	W32Time	None	64	N/A	STUDENT13	
		4/28/2003	3:32:09 PM	Browser	None	8035	N/A	STUDENT13	
		4/28/2003	3:27:15 PM	Browser	None	8015	N/A	STUDENT13	
	Warning	4/28/2003	3:27:09 PM	Dhop	None	1007	N/A	STUDENT13	

Audit Checklist (con't)

- 17) **EVENT LOGS** Verify that the configuration of the event logs will retain an appropriate amount of data (e.g. Max. log size & "Do not overwrite events", etc.).
 - Where? Start, Programs, Administrative Tools, Event Viewer, right click on each type of log and select Properties or Group Policy, Windows Settings, Event Log

Security Log Prope	erties ?X	🚮 Group Policy		
General Filter] Action ⊻iew] 🗢 → 🔁 [🖸 X 🛱 😫	
-		Tree	Policy A	Computer Setting
Display name:	Security Log	Default Domain Policy [student1:	BB Maximum application log size	Not defined
Log name:	D:\WINNT\System32\config\SecEvent.Evt	🗐 🌉 Computer Configuration	Maximum security log size	Not defined
Size: Created: Modified: Accessed: Log size Maximum log s When maximu © Overwrite o	192.0 KB (196,608 bytes) Sunday, April 27, 2003 3:46:21 PM Thursday, May 01, 2003 11:35:03 AM Thursday, May 01, 2003 11:35:03 AM size: 4032 KB m log size is reached: events as needed events older than 7 days erwrite events nanually) Restore Defaults	Software Settings Windows Settings Scripts (Startup/Shu Security Settings Security Settings Coal Policies Local Policies Local Policies Software Settings Software Settings	 Maximum system log size Restrict guest access to application log Restrict guest access to security log Restrict guest access to system log Retain application log Retain security log Retain system log Retention method for application log Retention method for system log Retention method for system log Retention method for system log Shut down the computer when the security a 	Not defined Not defined Not defined Not defined Not defined Not defined Not defined Not defined Not defined Not defined
	OK Cancel Apply			

Audit Checklist (con't)

18) **SHARES** – Verify that access to critical shared folders is appropriately controlled through Access Control Lists and Permissions.

 Where? – Start, Programs, Administrative Tools, Computer Management, double click on the critical shared folders and review the Security tab

Tree	Shared Folder	Shared Path	General Share Permissions Security	
4	And the second s	Shared Path A	Name	Add.
J Computer Management (Local) → System Tools →	erts	C:\ D:\ D:\Documents and Settings\Administrator\Desktop\pi sation D:\Executive Compensation D:\WINNT	Curly (Curly@dandt.com) Guest (SUBSIDIARY13\Guest) Internal Auditors (SUBSIDIARY13\Internal Auditors) Larry (Larry@dandt.com)	Remo
Shares		D:\WINNT\SYSVOL\sysvol D:\WINNT\SYSVOL\sysvol\subsidiary13.acme.local\S(Permissions: Allow	v Der
Device Manager Storage Disk Management Disk Defragmenter Logical Drives Removable Storage			Full Control Image: Control Modify Image: Control Read & Execute Image: Control List Folder Contents Image: Contents Read Image: Contents Write Image: Contents	
E - Services and Applications			Advanced Allow inheritable permissions from parent to propagate to object) this

Audit Checklist (con't)

19) **DRIVES MAPPED** – Verify the validity of mapped drives.

Where? – Start, Programs, Administrative Tools, Computer Management, select Logical Drives

ee	Name	Туре	Mapping	
Computer Management (Local) System Tools System Toformation Performance Logs and Alert Shared Folders Device Manager Local Users and Groups Storage Disk Management Disk Defragmenter Cogical Drives Removable Storage Services and Applications	A: C: D: & E:	31/2-Inch Floppy Disk Local Disk Local Disk Compact Disc	Local Local Local Local	



20) **LEGAL NOTICE** – Review the appropriateness of the Legal Notice within the Group Policy.

Where? – Start, Programs, Administrative Tools, Active Directory Users and Computers, right click on the Domain Controllers OU select properties then Group Policy. Select the GPO, click on Edit, then review the Security Options.

Action Yiew 🗍 🖛 🔿 🛛 🔁				
e	Policy 🛆	Computer Setting		
Default Domain Controllers Polic	/ [s 📴 Additional restrictions for anonymous connec	Not defined		
R Computer Configuration	Allow server operators to schedule tasks (do	Not defined		
🗄 🧰 Software Settings	Allow system to be shut down without havin	Not defined		
🗄 🧰 Windows Settings	Allowed to eject removable NTFS media	Not defined		
	tdo 📴 Amount of idle time required before disconne	Not defined		
🚊 🔂 Security Settings	Audit the access of global system objects	Not defined		
🗄 🛃 Account Policies	Audit use of Backup and Restore privilege	Not defined		
🖃 🚽 🛃 Local Policies	Automatically log off users when logon time			
Audit Policy	Automatically log off users when logon time			
User Rights	Clear virtual memory pagenie when system s	Not defined		
Security Opl	ion: 📴 Digitally sign client communication (always)	Not defined		
Event Log	Digitally sign client communication (when pos	Not defined		
😟 😥 😥 😥 😥 😥 😥 😥 😥 😥	Digitally sign server communication (always)	Not defined		
System Services		Enabled		
Registry	Disable CTRL+ALT+DEL requirement for logon	Not defined		
File System	BOD not display last user name in logon screen	Not defined		
🖅 🦳 Public Key Policie	LAN Manager Authentication Level	Not defined		
🗄 🥷 IP Security Polic		DEFINE WARNING BANNER HERE		
Administrative Template		DEFINE WARNING BANNER HERE		
User Configuration	Number of previous logons to cache (in case	Not defined		
🗉 🧰 Software Settings	Prevent system maintenance of computer ac	Not defined		
🗄 🧰 Windows Settings	Prevent users from installing printer drivers	Not defined		
🗄 🧰 Administrative Template	5 Being Prompt user to change password before expi	Not defined		
	Recovery Console: Allow automatic administr	Not defined		
	Recovery Console: Allow floppy copy and ac	Not defined		
	Rename administrator account	Not defined		
	Rename guest account	Not defined		
	Restrict CD-ROM access to locally logged-on	Not defined		
	Restrict floppy access to locally logged-on us	Not defined		
	Secure channel: Digitally encrypt or sign sec			
	Secure channel: Digitally encrypt secure cha	Not defined		
	Secure channel: Digitally sign secure channel	Not defined		
	Secure channel: Require strong (Windows 20	Not defined		
	Secure system partition (for RISC platforms			
	Send unencrypted password to connect to t			
	Shut down system immediately if unable to lo			
	Smart card removal behavior	Not defined		
	Strengthen default permissions of global syst			

Tools for Managing & Auditing Security

Checking & Managing Security Configuration Tools

Security Configuration & Analysis Tool Set

- Provided by Microsoft to compare current configuration vs. a security template
- The security template defines almost all security settings for Windows 2000
- Various templates can be customized per each type of system or level of security

Microsoft Baseline Security Analyser

- Provided by Microsoft to compare configuration for the latest security related hofixes, service packs, and performs an analysis of various common security misconfigurations
 - Windows
 - IIS
 - SQL
 - Desktop application

CIS's Benchmarks and Scoring Tool (www.cisecurity.org)

- A consensus of CIS members (SANS, NSA, DISA, NIST, & GSA)
- A compilation of security configuration actions and settings that "harden" the Windows O/S

4

- "the minimum level of due care"
- "unlikely to cause an interruption of service"

Tools for Managing & Auditing Security (con't)

Reporting Security Configuration Tools

- Microsoft doesn't provide built-in reporting capabilities, therefore gathering evidence supporting audit findings is very difficult & time consuming
- Windows 2000 security management and auditing is impractical without the use of third party reporting tools
- A few Reporting/Auditing Tools
 - DumpSEC (www.systemtools.com)
 - A free tool that provides the major security reports needed for auditing users, group policy, services, rights, shares and permission reports
 - Can only be processed on one domain or system at a time and requires administrator access

SekCheck

 Endorsed and used by D&T to extract, report, and audit system configurations from Domain Group Policy settings to Home Directories, Logon scripts, and Profiles

4

Results are processed within 24 hours

Various others Tools

Tools for Managing & Auditing Security (con't)

Security Log Analysis Tools

- DumpEL
 - Part of Windows 2000 resource kit

ELDump

- Freeware which is more versatile and faster than DumpEL and contains better filtering options
- Best for reporting directly form the security logs

DumpEVT

- Handles special characters better than DumpEL to prevent problems with importing
- There is no filtering available, therefore it is most commonly used to import into Access

NTLast

Used for analyzing logon activity from the security logs

Useful Resources

Publications

- Hacking Windows 2000 Exposed
 - ◆ Joel Scambray, Foundstone

Hack Proofing Windows 2000 Server

Chad Todd

Web Sites

- MS Security Bulletins
 - www.microsoft.com/security
- www.ntsecurity.net
- www.win2000mag.com
- www.websolutions.com
- www.winnetmag.com
- www.labmice.net/Security/
- www.sunbeltsoftware.com

Forums

- www.ntbugtraq.com
- www.secadministrator.com/forums/