



Information Systems
Audit and Control
Association®

< FOCUS > < DISCOVER > < INTEGRATE > < ADVANCE >

Auditing in a Windows Environment

Presented By:
Nicholas Green

The San Francisco Chapter of ISACA Proudly Announces the 4th Annual:

2004 SF ISACA FALL CONFERENCE

October 4-6, 2004

Agenda

◆ Session 1

- Introduction to Windows
- Windows Security Controls

◆ Session 2

- Active Directory
- Access Controls

◆ Session 3

- Host Security
- Auditing Windows

Session 1 Agenda

- ◆ Introduction to Windows
- ◆ Active Directory
- ◆ File systems
- ◆ Network support
- ◆ Services
- ◆ The registry
- ◆ Security Identifier
- ◆ Event Logs
- ◆ Windows Security Controls

Introduction to Windows

- ◆ Windows 200x is based on the NT security model
- ◆ Well-defined discretionary access control framework

Introduction to Windows Authentication techniques

◆ NTLM authentication

- Backward compatibility with previous versions of Windows.
- Weakness – sniff message hash and crack password

Introduction to Windows

Authentication techniques

- ◆ Secure Sockets Layer/Transport Layer Security (SSL/TLS)
- ◆ Digest authentication
- ◆ Strong authentication
 - i.e. two factor authentication (e.g. smart cards)

Introduction to Windows Authentication techniques

- ◆ Kerberos V5 authentication
 - Default method of authentication between W2k systems
 - Provides for mutual authentication
 - Between a client and a server, or between one server and another,
 - Without sending data across the network that might allow the principal to be impersonated

Introduction to Windows

“Least privilege” principle

- ◆ Minimum set of rights and privileges necessary to perform assigned function
- ◆ Delegation
 - Administration privilege is no longer all or nothing
 - Any privilege can be delegated
 - Privilege can apply to all objects or a subset of objects

Active Directory

- ◆ **What is a Directory Service?**
- ◆ An information source used to store information about objects

Active Directory

Why Have a Directory Service?

- ◆ Allow users and administrators to find objects
- ◆ Enforce security to keep information safe from intruders
- ◆ Distribute the directory across many computers in a network

Active Directory

Why Have a Directory Service?

- ◆ Replicate the directory to make it available to more users and resistant to failure
- ◆ Partition a directory into multiple stores to allow the storage of a very large numbers of objects

Active Directory

What Is the Active Directory?

- ◆ The directory service included with Windows 200x

Active Directory Domains

- ◆ **The core unit of logical structure in Active Directory**
- ◆ The boundary of
 - Security
 - Authentication
 - Replication
 - Administration

File systems

- ◆ **FAT/FAT32**
- ◆ No reason to use
- ◆ **NTFS v5**
- ◆ Default file system
- ◆ Allows granular control and monitoring of files
- ◆ Insert screenshot

File systems

Encrypting File System (EFS)

- ◆ Not a file system in itself
- ◆ An integral part of NTFS v5
- ◆ Encrypts files using unique key per file
- ◆ Transparent to users and applications

File systems

Encrypting File System (EFS)

- ◆ Need to consider key management/recovery
- ◆ Enterprise data recovery using public key technology (a subset of Group Policy)
- ◆ Recovers individual file encryption key, not user's encryption key

Network support

- ◆ TCP/IP is the core networking protocol
- ◆ Integral part of OS in some versions (XP / 2003)
- ◆ Cannot be uninstalled

Network support

◆ Many others:

- Netbios
- NetBEUI (Windows for Work groups)
- IPX/SPX (Novell)
- Appletalk

Services

- ◆ A process or set of processes that adds functionality to Windows by providing support to other programs
- ◆ The default installation of each version of Windows provides a core set of services and configurations designed to suit most needs, while offering users some flexibility

Services

- ◆ Every service has three user controllable states:
 - Disabled. Installed but not currently running.
 - Manual. Installed but starts only when another service or application needs its functionality.
 - Automatic. Started by the operating system after device drivers are loaded at boot time.

The registry

- ◆ A central hierarchical database to store system configuration information
 - User profiles
 - Applications installed
 - Document types
 - Hardware on the system
 - Ports that are being used

Security Identifier (SID)

- ◆ Uniquely identifies user, group, and computer accounts
- ◆ When the account is deleted, the SID is destroyed
- ◆ Thus if an account is created with the same name, it will not assume any of the previous account's permissions

Security Identifier (SID)

Well Known Security Identifiers

Knowledge Base Article – 243330

- ◆ SID: S-1-1-0
- ◆ Name: Everyone
- ◆ Description: A group that includes all users, even anonymous users and guests. Membership is controlled by the operating system.

Security Identifier (SID)

Well Known Security Identifiers

Knowledge Base Article – 243330

- ◆ SID: S-1-5-domain-500
- ◆ Name: Administrator
- ◆ Description: A user account for the system administrator. By default, it is the only user account that is given full control over the system.

Security Identifier (SID)

Well Known Security Identifiers

Knowledge Base Article – 243330

- ◆ SID: S-1-5-32-544
- ◆ Name: Administrators
- ◆ Description: A built-in group. After the initial installation of the operating system, the only member of the group is the Administrator account.

Event Logs

Standard Event Logs

◆ Application log

- Errors, warnings, and informational messages generated by application software
- Can be written to and read by any user

◆ System

- Errors, warnings, and informational messages generated by the OS
- Can be written to and read by any user

Event Logs

Standard Event Logs

◆ Security

- Errors, warnings, and informational messages about security events
- Members of the local Administrators group have read access
- Write access is limited to processes that are running in the security context of the Local System or to an Administrator

Event logs

Specialized Event Logs

◆ Directory Service Log

- Errors, warnings, and informational messages about the operation of Active Directory
- Can be read by any user
- Only exists on domain controllers

◆ DNS Server Log

- Errors, warnings, and informational messages about the operation of an installed DNS server
- Can be read by any user
- Only on Windows servers running the DNS service

Event logs

Specialized Event Logs

◆ File Replication Service Log

- Errors, warnings, and informational messages about the operation of the File Replication Service
- Can be read by any user
- Only exists on Win2K servers that are running the FRS

Windows Security Controls

Account policies

- ◆ Located in the following Group Policy path:
 - Computer Configuration, Windows Settings, Security Settings
- ◆ Account policy options
 - Password security
 - Account Lockout
 - Kerberos security

Windows Security Controls

Password policy

- ◆ Enforce password history
 - Requires users to choose new passwords when they make a password change
- ◆ Maximum password age
 - Sets maximum time before password expires
 - Commonly 45 to 90 days
- ◆ Minimum password age

Windows Security Controls

Password policy

- ◆ Minimum password length
 - A minimum of seven characters for a “strong password”
- ◆ Password must meet complexity requirements
 - Filter of customized password requirements
- ◆ Store passwords using reversible encryption

Windows Security Controls

Lockout policy

- ◆ Account lockout threshold
 - The number of unsuccessful attempts to log on to an account
- ◆ Account lockout duration
 - How long the system keeps an account locked out after reaching the specified number of unsuccessful logon attempts (in minutes)
- ◆ Reset account lockout counter after
 - How soon to reset the unsuccessful logon counter (in minutes)

Windows Security Controls

Kerberos policy

- ◆ Enforce user logon restrictions
 - Turns on Kerberos security, which is the default
- ◆ Maximum lifetime for a service ticket
 - Maximum time in minutes that a ticket can access a particular service in one service session
- ◆ Maximum lifetime for a user ticket
 - Maximum time in hours that a ticket can be used in one continuous session for access to a computer or domain

Windows Security Controls

Kerberos policy

- ◆ Maximum lifetime for user ticket renewal
 - Maximum number of days that the same Kerberos ticket can be renewed each time a user logs on
- ◆ Maximum tolerance for computer clock synchronization
 - Length in minutes a client waits until synchronizing its clock

Windows Security Controls

User Rights

- ◆ Enable an account or group to perform predefined tasks such as:
 - Access a server
 - Create accounts
 - Manage server functions
- ◆ Assign user rights to groups instead of to individual user accounts
 - Members of a group inherit the user rights of the group

Windows Security Controls

Audit policy

- ◆ Logon and Logoff
- ◆ File and Object Access
- ◆ Use of User Rights
- ◆ User and Group Management
- ◆ Security Policy Changes
- ◆ Restart, Shutdown, and System
- ◆ Process Tracking

Session 2 Agenda

- ◆ **Active Directory**
- ◆ **Resource Access Controls**
- ◆ **Group Policy**
- ◆ **Group Policy Management Console**
- ◆ **Cross Forest Trusts**
- ◆ **Server 2003 Secure by Default**

Active Directory

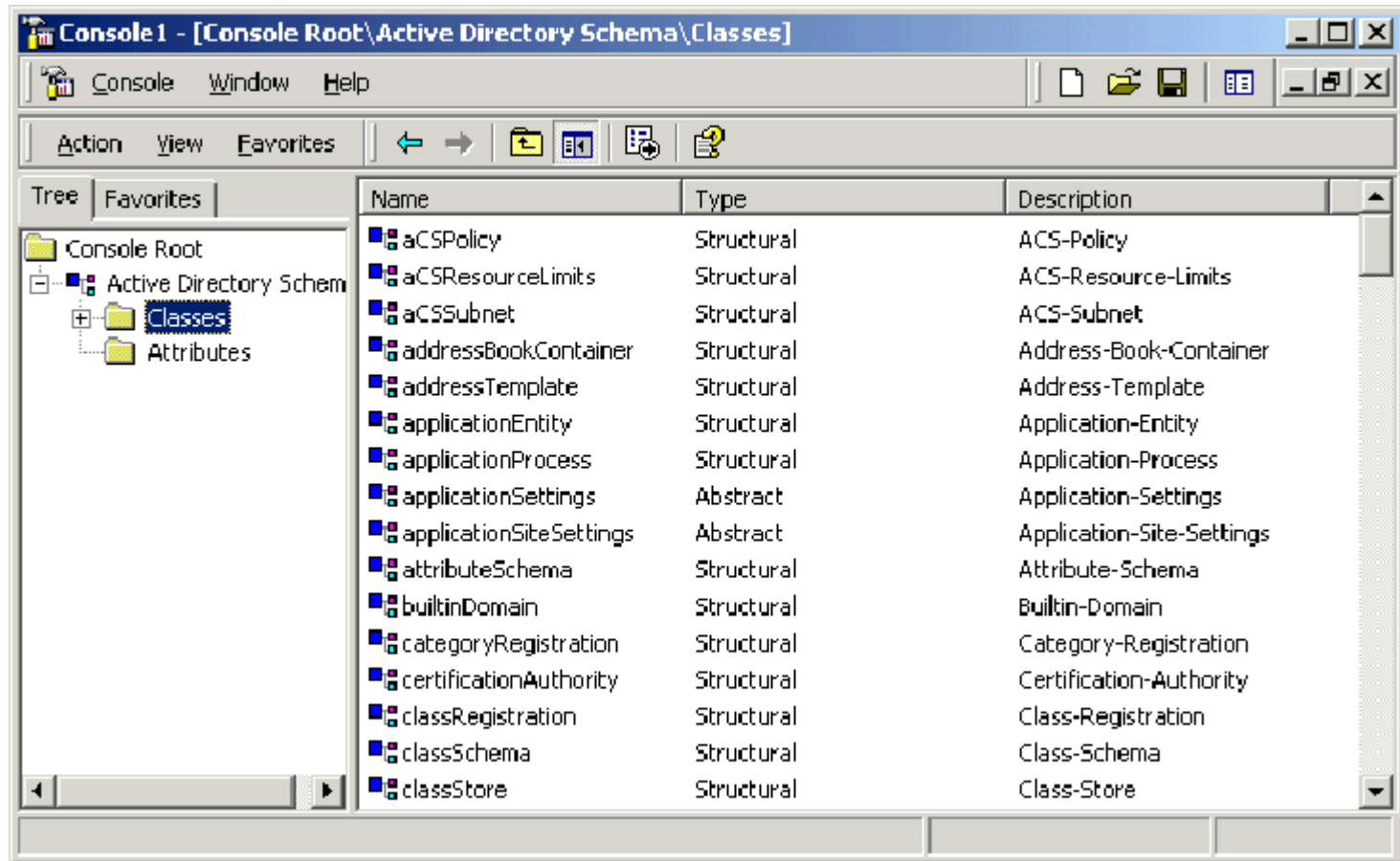
- ◆ Core of Windows 200x security
- ◆ Replaces the security accounts manager (SAM) database of Windows NT
- ◆ Stores user information to support both authentication and access control functions

Active Directory

Objects and Attributes

- ◆ Primary item of storage in AD is an *object*.
 - E.g. users, computers, and printers
 - Other items e.g. policies are also stored as objects
- ◆ There is a set of *classes*, to define the objects one can create
- ◆ Each class has a set of *attributes*
 - The user class has attributes First Name, Address, etc
- ◆ The underlying dictionary of classes and their attributes is referred to as the *schema*

Active Directory



Active Directory

- ◆ Orders objects in an hierarchical structure
- ◆ Integrates the Internet Domain Name System (DNS) concept of a namespace
- ◆ Every object in a Windows AD environment has a unique name within the Active Directory hierarchical namespace

Active Directory Domains

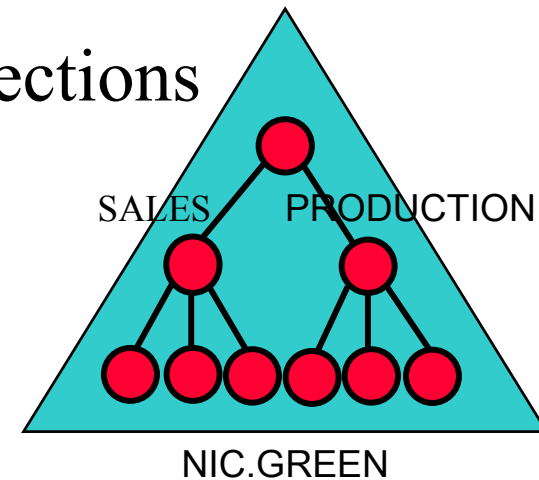
- ◆ **Core unit of logical structure**
- ◆ **Boundary of Security and Control**
- ◆ **Boundary of Replication**
- ◆ **Boundary of DNS Namespace**
- ◆ **Boundary of Administration**



Active Directory

Organizational Units

- ◆ Containers within Domains
 - Can define a logical hierarchy within the directory without creating additional domains
- ◆ Distinct Units of Administration
 - Subdivide domains into discrete sections and delegate administrative duties
- ◆ Unique to Domains

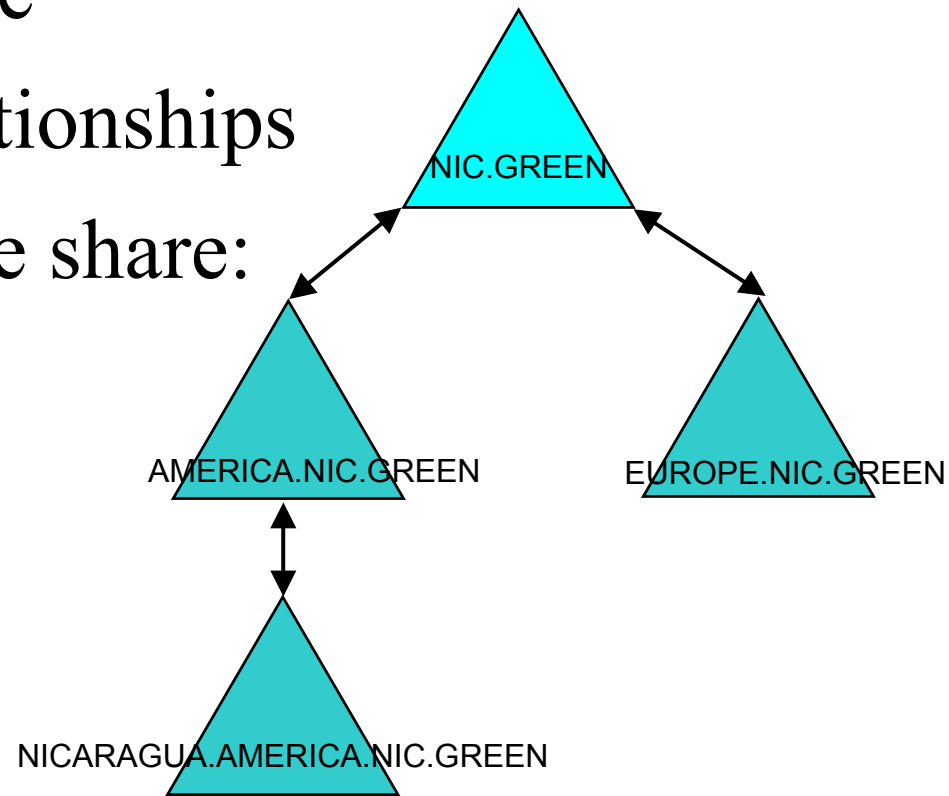


Active Directory Trusts

- ◆ Defined between Windows domains
- ◆ Allows users in one domain to be authenticated by servers in another domain
- ◆ All domains within a domain tree are linked by two-way transitive trust relationships
 - If domain A trusts domain B and domain B trusts domain C, then domain A trusts domain C and vice versa
- ◆ Windows automatically creates a two-way trust, using a secret key shared by the parent and child domains
- ◆ Two-way transitive trust relationships exist between all domains in a tree

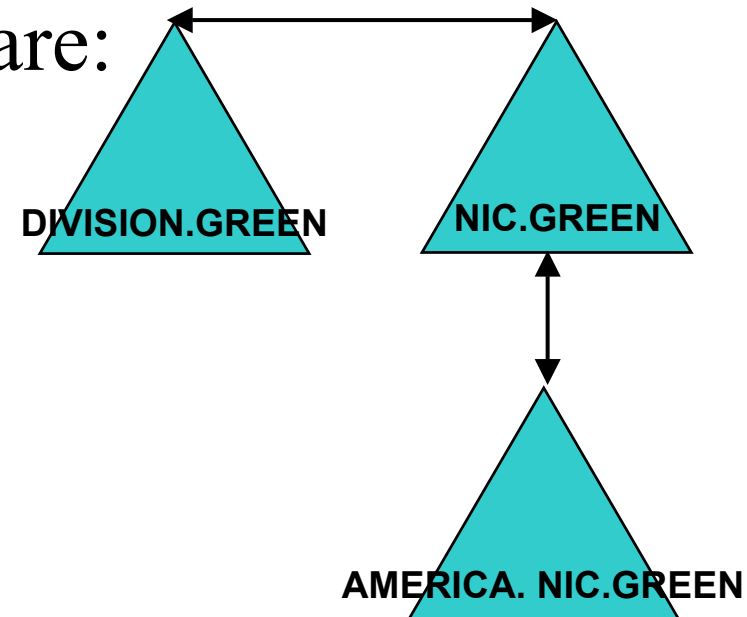
Active Directory Trees

- ◆ Hierarchy of Domains forming a contiguous namespace
- ◆ Transitive Trust Relationships
- ◆ All Domains in a Tree share:
 - Schema
 - Configuration
 - Global Catalog



Active Directory Forests

- ◆ Hierarchy of Domains forming a contiguous or disjoint namespace
- ◆ Transitive Trust Relationships
- ◆ All Domains in a Forest share:
 - Schema
 - Configuration
 - Global Catalog



Active Directory

Built-in Groups

- ◆ Groups are AD objects that represent collections of users and computers
- ◆ Primary means of implementing user security
 - A universal group can contain users and groups from any domain and can be used for access control in any domain
 - A global group contains users and groups from a single domain but can be used for access control on any domain
 - A domain local group can contain users and groups from any domain and can only be used for access control within a single domain
- ◆ Windows creates certain groups at installation

Active Directory

Built-in Groups - Global Groups

- ◆ Global groups provide the ability to assign users to authorized administrator and authorized user roles with unique domain level access restrictions based on the global group to which the user is assigned.
- ◆ Domain Admins
Only on Domain Controllers, members have administrative privileges for the entire domain.
Default Members – local Administrator
- ◆ Domain Computers
All servers and workstations in the domain, except domain controllers.
- ◆ Domain Guests
Only on Domain Controllers, members may only access the system from the network and have very limited privileges.
Default Members – Guest account
Do not use this group. Remove all accounts including Guest from this group.

Active Directory

Built-in Groups - Global Groups

◆ Domain Users

Only on Domain Controllers.

A member of the Users local group for the domain and for every Windows computer in the domain.

Default Members – Administrator, Guest, Krbtgt, TsInternetUser, all new users are added by default.

Remove the Guest, and TsInternetUser accounts.

◆ Enterprise Admins

Members have administrative control over the entire network and may make forest-wide changes in Active Directory, such as adding child domains.

Default Members – Domain Controller's Administrator.

◆ Group Policy Creator Owner

Members can modify or create new group policy for the domain.

Default Members – Administrator

Active Directory

Built-in Groups - Domain Local Groups

- ◆ Domain local groups provide users with privileges and permissions to perform tasks specifically on the domain controller and in the Active Directory store.
- ◆ **Account Operators**
Only on Domain Controllers. Members may administer user and group accounts for systems and domains.
Default Members – none.
- ◆ **Administrators**
Members can perform all administrative tasks on all domain controllers and the domain itself.
Default Members – Administrator, Domain Admins, Enterprise Admins
- ◆ **Backup Operators**
Members can back up and restore files on all domain controllers using Windows Backup, regardless of the file permissions. And can also log on to the computer and shut it down.
Default Members – none

Active Directory

Built-in Groups - Domain Local Groups

- ◆ **DnsAdmins**
Members have Full Control over a DNS Server and its zones.
Default Members – None
- ◆ **Guests**
Members have limited access to resources and cannot make permanent changes to their desktop environment. Some services add users to this group, e.g., IIS adds anonymous user accounts to the Guests group.
Do not use this group. Remove all accounts including Guest from this group.
- ◆ **Server Operators**
Only on Domain Controllers. Members can perform server management tasks e.g. creating, changing, and deleting shared printers, shared directories, and files. They can back up and restore files, lock the server console and shutdown the system. They cannot modify system policies or start and stop services.

Active Directory

Built-in Groups – Domain Local Groups

◆ Users

Members have the necessary rights to operate the computer as an end user, such as running applications and managing files. By default, Windows adds all new local user accounts to the Users group. Default Members – Authenticated Users, Domain Users, INTERACTIVE, all new local users are added by default.

Active Directory

Built-in Groups - Local Groups

- ◆ All stand-alone Windows Servers, (domain) member servers, and Windows 2000 Professional+ workstations have built-in local groups. These groups provide members with the capability to perform tasks on the specific computer
- ◆ **Administrators**
Members have complete control over the entire computer. When a server or a computer running Windows 2000+ joins a domain, the Domain Admins group is added to the local Administrators group. Default Members – Administrator, Domain Admins.
- ◆ **Backup Operators**
Members can use Windows Backup to back up and restore the computer regardless of file system security.

Active Directory

Built-in Groups - Local Groups

◆ Guests

Provides limited access to resources on the system. Members cannot make permanent changes to their desktop environment.

Default Members – the Guest user account for the computer. This account is disabled by default.

Do not use this group. Remove all accounts including Guest from this group.

◆ Power Users

Members have the ability to create and modify local user accounts on the computer and share resources, without giving the user complete control over the computer.

Default Members – none.

◆ Users

Provides the user with the necessary rights to operate the computer as an end user, such as running applications and managing files.

Default Members – Authenticated Users, Domain Users, INTERACTIVE, All new local users are added by default.

Active Directory

Built-in Groups - System Groups

- ◆ System groups do not have specific memberships that can be modified. Each represents a class of users or the operating system, are created automatically by Windows, but are not shown in the group administration GUIs.
- ◆ Anonymous Logon
Any user accounts that Windows did not authenticate.
- ◆ Authenticated Users
All users with a valid user account on the computer or in Active Directory.
- ◆ Everyone
All users who access the computer. Windows authenticates a user who does not have a valid user account as Guest and grants the user all permissions assigned to the Everyone group.
**Do not assign resource permissions or user rights to this account.
Use Authenticated Users or specific user accounts and groups**

Active Directory

Built-in Groups - System Groups

- ◆ **SERVICE**
All security principals logged on as a service.
- ◆ **SYSTEM**
Account used by the operating system to run services, utilities, and device drivers.
This account has unlimited power and access to resources that even Administrators are denied, such as the Registry's SAM.

Resource Access Controls

Access Control Lists

- ◆ Resource types: Active Directory objects, files, folders, shares, printers, registry keys
- ◆ Each object has a unique ACL which controls access to the object
- ◆ An ACL is made up of ACEs (access control entries) (i.e. the object's permissions)
- ◆ Two types of ACL
 - DACLs (Discretionary ACLs) for access
 - SACLs (System ACLs) for auditing

Resource Access Controls

Can I access file X?

- ◆ Windows looks for an explicit match between the requestor and the object
- ◆ First searches for a deny ACE
- ◆ Then searches for an allow ACE
- ◆ If no match is found, access is denied

Resource Access Controls Inheritance

- ◆ Default is for subordinate objects to inherit permissions
- ◆ Can be disabled
- ◆ Inheritance is determined dynamically at the time of object access

Resource Access Controls

Object Ownership

- ◆ Ownership can be assigned as well as taken allowing an attacker to:
- ◆ Take ownership of an object
- ◆ Change the object
- ◆ Assign ownership to original owner
- ◆ Ensure auditing is enabled for sensitive objects (and logs reviewed)

Group Policy

- ◆ Key tool for managing Windows security and configuration
- ◆ GP's can be used to
 - Change registry values
 - Perform software installation and maintenance
 - Replace user-based logon scripts
 - Redirect folders and data storage
 - Control security options

Group Policy

- ◆ Settings are contained in Group Policy Objects (GPO)
- ◆ Delivered by Active Directory
- ◆ GPO's are associated with AD containers
 - Local computer
 - Site
 - Domain
 - Organizational Unit

Group Policy

- ◆ GPO is applied in the following order:
 - Local GPO
 - Site GPO
 - Domain GPO
 - Organizational Unit GPO (from parent to children)
- ◆ In addition you can set GPO
 - Inheritance Blocking and
 - Enforce (Override Inheritance Blocking)

Group Policy Management Console

- ◆ Requires Server 2003 or XP SP1 (Windows 2000 only supports Group Policy Editor and requires you to have edit access to the GPO)
- ◆ Create and edit GPOs.
- ◆ Link GPOs to sites, domains, or OUs.
- ◆ Delegate permissions on GPOs
- ◆ Determine the resultant set of policy (i.e. which policy will actually “win”)

Group Policy Management Console

- ◆ Backup, Restore, and Import GPOs
- ◆ Move GPOs between Domains and Forests
- ◆ Determine the Resultant Set of Policy
- ◆ Report GPO Settings and Resultant Set of Policy
- ◆ Only need Read permissions on the GPO to product a report and review its settings

Cross Forest Trusts

- ◆ Server 2003 supports cross-forest trusts
- ◆ Enables the explicit trust of certain, or all, users or groups in another Active Directory
- ◆ E.g. to allow access by a business partner's users

Server 2003 Secure by Default

- ◆ Secure root ACL to stop access to root directory (c:\)
- ◆ Changed default share ACL from Everyone:F to Everyone:R
- ◆ Changed DLL Search Order to start in system directory
- ◆ Hardened Internet Explorer
- ◆ Anonymous users are no longer members of “Everyone” by default.

Server 2003 Secure by Default

- ◆ Local accounts with blank passwords cannot be used to remotely connect to computers
- ◆ Server 2003 will not send insecure LanMan responses (LanManCompatibilityLevel=2 registry setting on Servers\DCs)
- ◆ Restricted remote execution of console apps to admins only

Server 2003 Secure by Default

- ◆ Two new accounts to run services with lower privileges than system
- ◆ Network Service
 - DHCP Client
 - Distributed Transaction Coordinator
 - DNS Client
 - License Logging
 - Performance Logs and Alerts
 - RPC Locator

Server 2003 Secure by Default

◆ Local Service

- Alerter
- Application Layer Gateway Service
- Remote Registry
- Smart Card
- Smart Card Helper
- SSDP Discovery Service
- TCP/IP NetBIOS Helper
- Telnet
- UPS
- Universal Plug and Play
- Web Client
- Windows Image Acquisition
- WinHTTP Web Proxy Auto-Discovery Service

Server 2003 Secure by Default

◆ Services Turned Off by Default

- IIS not installed by default
- Alerter
- Clipbook
- Distributed Link Tracking Server
- Human Interface Device Access
- Imapi CDROM Burning Service
- ICF\ICS
- Intersite Messaging
- License Logging
- Messenger
- NetMeeting Remote Desktop Sharing
- Network DDE
- Network DDE DSDM
- Routing and Remote Access
- Telnet
- Terminal Service Session Discovery
- Themes
- WebClient
- Windows Image Acquisition (WIA)
- Kerberos KDC (automatically enabled upon DCPromo)

Server 2003 Secure by Default

- ◆ New IIS 6.0 architecture
- ◆ Software restriction policies
 - Server 2003 and XP only
 - Restrict a specific version
 - Restrict a file type
 - Restrict installation of executables

Session 3 Agenda

- ◆ **Server Host Security**
- ◆ **Collecting Evidence**
- ◆ **Tools**
- ◆ **Auditing Windows Server**

Server Host Security

Consider

- ◆ Physical access to servers
- ◆ Network access to servers – Logon from Network privilege
- ◆ Services logging on using a domain account
- ◆ OS2 and POSIX should be disabled
- ◆ Password policies

Server Host Security

Consider

- ◆ Disable LAN Manager and NTLMv1 authentication
- ◆ Services that are not required
- ◆ Service Pack and security patch levels
- ◆ Administrator and Guest accounts renamed

Server Host Security

LAN Manager and NTLMv1

- ◆ To disable requires
 - SP4 on all NT 4.0 clients
 - Directory services client on all Windows 95 or 98 clients
- ◆ Domain Group Policy for LAN Manager Authentication Level should be:
Send NTLMv2 response only\refuse LM & NTLM
 - Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\

Server Host Security

Services You Should Not Disable

- ◆ Cryptographic Services
- ◆ DHCP Client
- ◆ DNS Client
- ◆ Event Log
- ◆ IPsec Services
- ◆ Netlogon
- ◆ NTLM Security Support Provider
- ◆ Plug and Play
- ◆ Protected Storage
- ◆ Remote Procedure Call (RPC)
- ◆ Remote Registry Service
- ◆ Security Accounts Manager
- ◆ Server System Event Notification
- ◆ TCP/IP NetBIOS Helper
- ◆ Windows Installer
- ◆ Windows Management Instrumentation
- ◆ Windows Time
- ◆ Workstation

Server Host Security

Services that can be Disabled

- ◆ ClipBook
- ◆ Error Reporting Service
- ◆ HTTP SSL
- ◆ IMAPI CD-Burning COM Service
- ◆ Indexing Service
- ◆ Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS)
- ◆ Messenger
- ◆ Microsoft POP3 Service
- ◆ NetMeeting Remote Desktop Sharing
- ◆ Remote Access Auto Connection Manager
- ◆ Remote Access Connection Manager
- ◆ World Wide Web Publishing Service

Server Host Security

Service packs and security patches

- ◆ Add/Remove programs
- ◆ Administration tools:
 - Microsoft Baseline Security Analyzer (MBSA)
 - HFNetChk
 - Software Update Services (SUS)
 - Systems Management Server (SMS)

Collecting Evidence Manual

- ◆ Print screen / notes
 - Point audits (e.g. password settings)
 - Single/limited number of servers
 - Small domain
 - No choice (tools not permitted)
- ◆ Effective for limited scale/scope audit
- ◆ Does not scale

Collecting Evidence Tools

- ◆ Windows standard utilities
- ◆ Windows 200x resource kit utilities
- ◆ Shareware / freeware utilities
- ◆ Commercial products
 - Symantec ESM
 - BindView
- ◆ Efficient and reliable
- ◆ Installation can be complex
- ◆ Commercial \$\$\$

Collecting Evidence Scripts

- ◆ Automation of both registry review and running tools
- ◆ Allows administrator to review exact actions
- ◆ Requires installation of scripts and tools on the local server
- ◆ Requires running as at least local administrator

Collecting Evidence

Script Example

- ◆ echo ***** >> ..\tmp\%1_1.txt
- ◆ echo Local account and password policy >> ..\tmp\%1_1.txt
- ◆ net accounts >> ..\tmp\%1_1.txt

- ◆ echo ***** >> ..\tmp\%1_1.txt
- ◆ echo NTLM version (Q239869 - <http://support.microsoft.com>) >> ..\tmp\%1_1.txt
- ◆ echo Recommended: REG_DWORD lmcompatibilitylevel 1 >> ..\tmp\%1_1.txt
- ◆ echo Preferred: REG_DWORD lmcompatibilitylevel 5 >> ..\tmp\%1_1.txt
- ◆ echo. >> ..\tmp\%1_1.txt
- ◆ reg query
HKLM\system\currentcontrolset\control\lsa\lmcompatibilitylevel
>> ..\tmp\%1_1.txt
- ◆ echo. >> ..\tmp\%1_1.txt

Tools

Windows Standard Utilities

- ◆ cacls – display ACL's
- ◆ Nbtstat – NETBIOS details
- ◆ net
 - Current password parameters
 - Global groups (on DC's only)
 - Local groups
- ◆ Netstat - displays protocol statistics and current TCP/IP network connections
- ◆ secdit – analyze system security based on a predefined security template
- ◆ set – lists environment variables

Tools

Windows Standard Utilities

◆ Group Policy Management Console

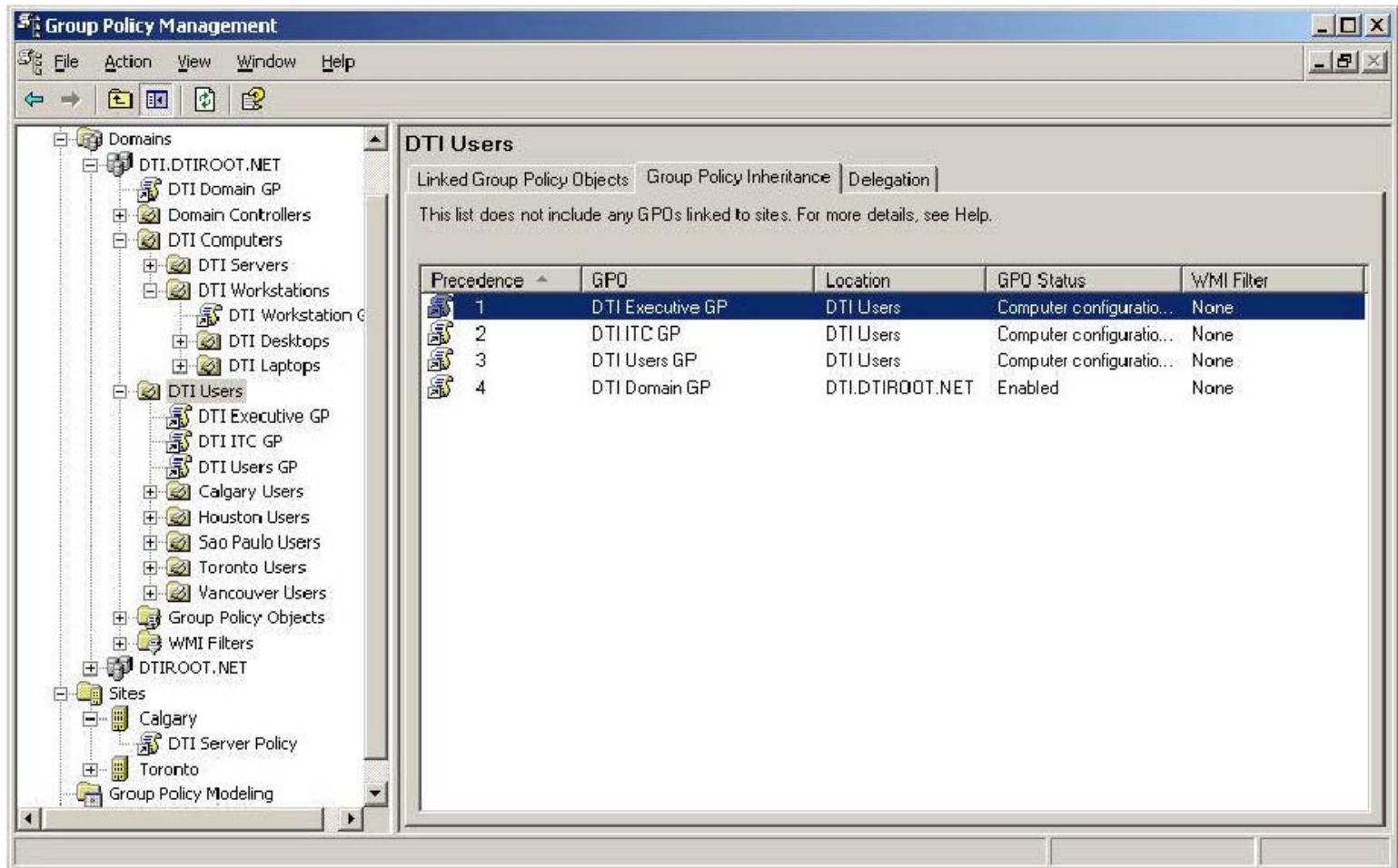
- <http://www.microsoft.com/windowsserver2003/downloads/featurepacks/default.mspx>

◆ Once installed, launch from

- Start\Programs\Administrative Tools\Group Policy Management
- or run GPMC.msc

Tools

Windows Standard Utilities



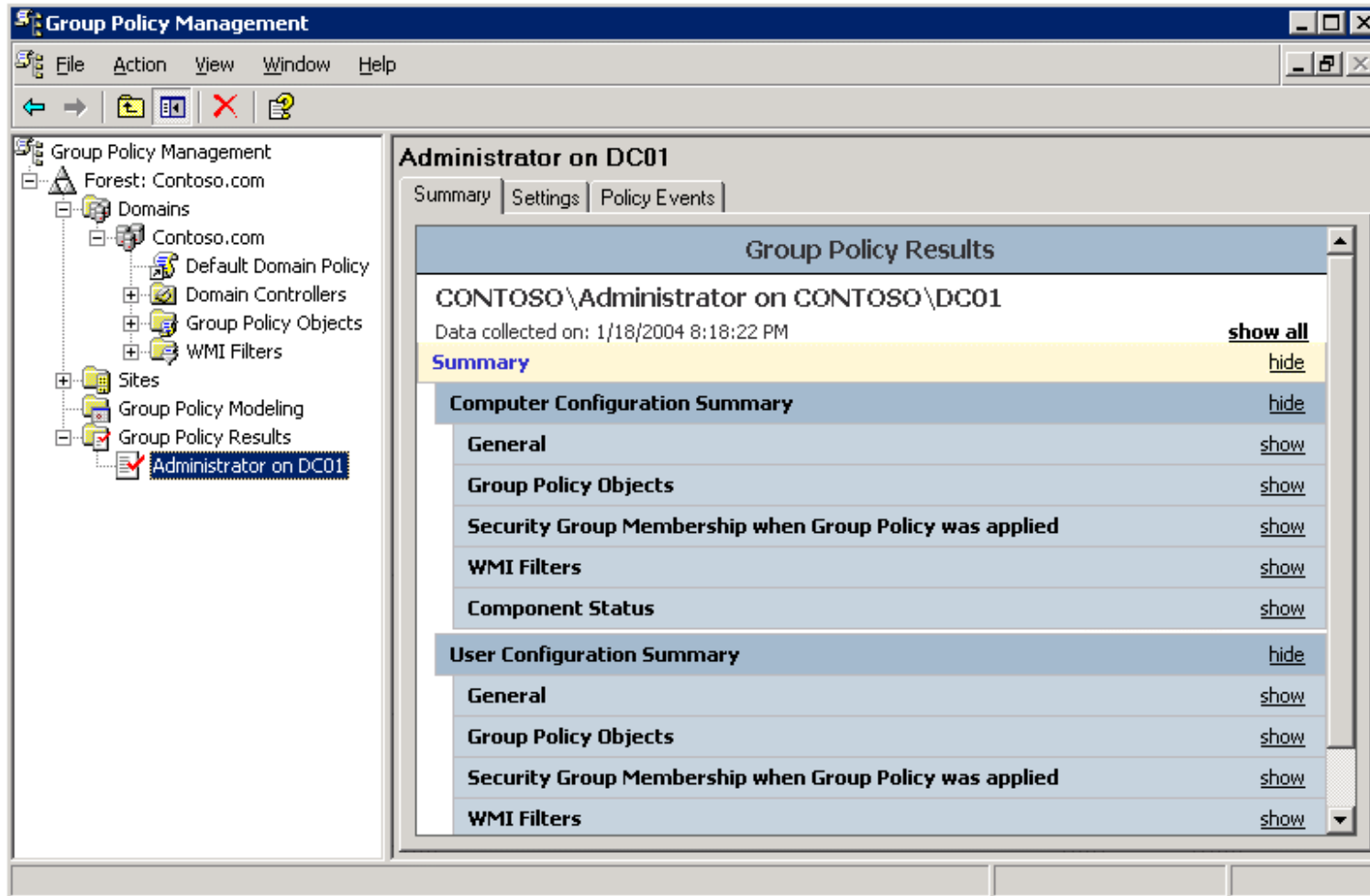
Tools

Windows Standard Utilities

- ◆ GPMC Settings Tab
- ◆ The most useful display in the GPMC
- ◆ HTML report of all the configured settings within a GPO
- ◆ Individual section can be expanded
- ◆ Report can be saved in HTML or XML, or printed

Tools

Windows Standard Utilities



Tools

Windows resource kit utilities

- ◆ AuditPol – Query audit policy
- ◆ Gpmonitor.exe – reports on GPO's based on a security template
- ◆ GPOTool – list online domain controllers all GPOs in the domain
 - lists all controllers currently online
- ◆ passprop – Password strength settings (in NETMGT.CAB on W2k)
- ◆ Perms – display user access permissions for a file or directory
- ◆ QueryAD – Query the AD for objects matching the name you specify and display the mandatory and optional properties of the object and of any child objects

◆ reg query – query a registry key

October 6, 2004

Presented by:
Nicholas Green

90

Tools

Shareware/Freeware Utilities

◆ DumpWin.exe

Parameters :

- i : List installed Programs.
- s : System Information.
- h : List shares present.
- p : List active Processes.
- g : List Local Group Accounts
- l : dumpACL
- a : All of above.
- d : Drive Information.
- m : Check for Modem Drivers.
- t : List Startup Programs.
- v : List of Services.
- u : List User Accounts.
- n : Account Lockout Policy

Tools

Shareware/Freeware Utilities

- ◆ FPort.exe – Maps TCP/IP Processes to Ports
- ◆ Fscan.exe – Port scanner
- ◆ NetPWAge.exe – Password age for user and machine accounts in the specified domain
- ◆ GPList.exe – lists GPO's in the order they are applied
- ◆ CIS-Win – CIS Benchmarks, supports NT – 2003 and has benchmarks for workstations and servers

Tools

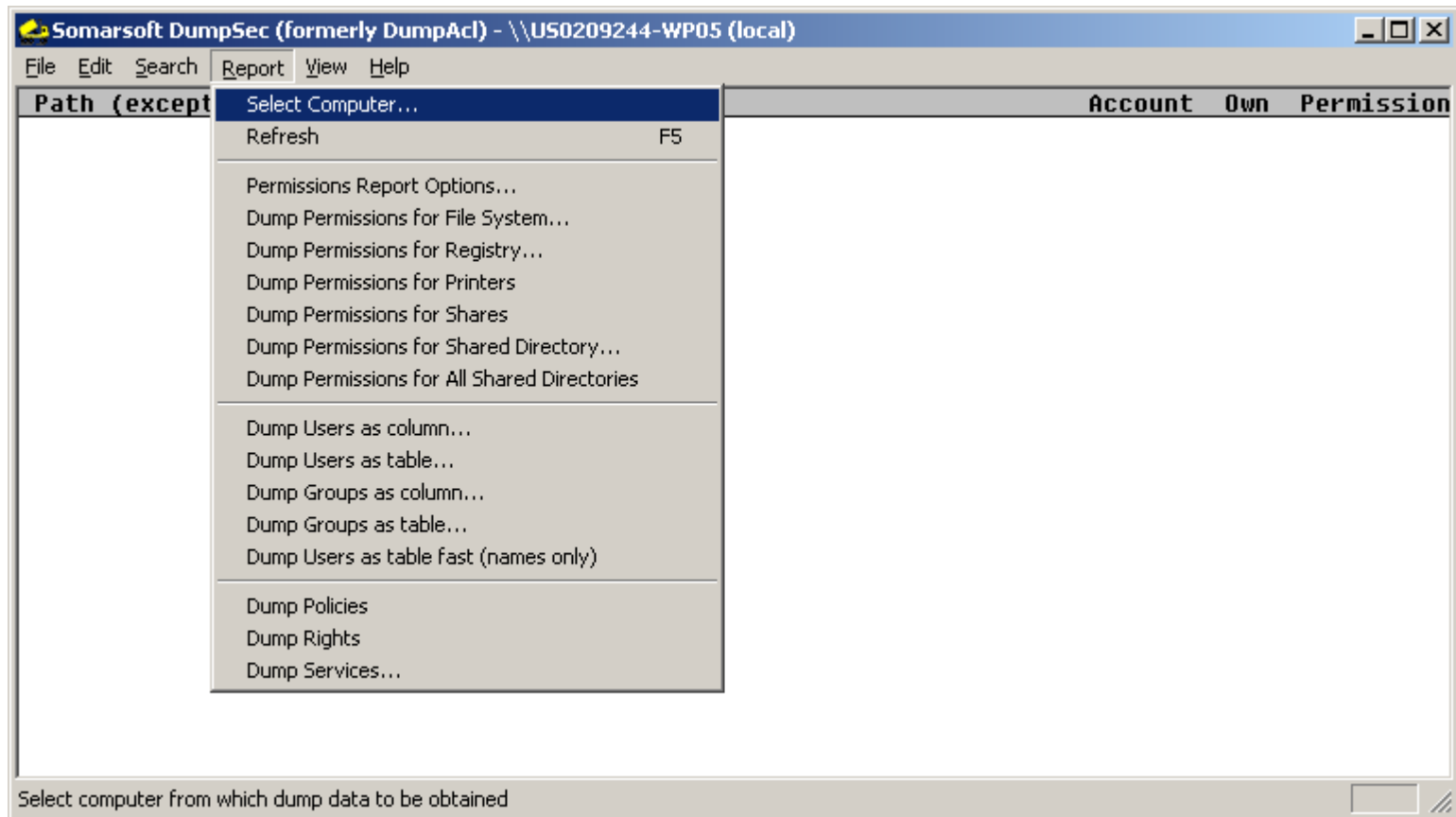
Shareware/Freeware Utilities

- ◆ **Microsoft Baseline Security Analyzer - MBSA (command line version mbsacl, if using scripts)**
 - Password weaknesses
 - Guest account not disabled
 - Auditing not configured
 - Unnecessary services installed
 - IIS vulnerabilities
 - IE zone settings
 - Automatic Updates configuration
 - Internet Connection Firewall configuration
 - Missing security patches
 - Potential configuration issues

Tools

Shareware/Freeware Utilities

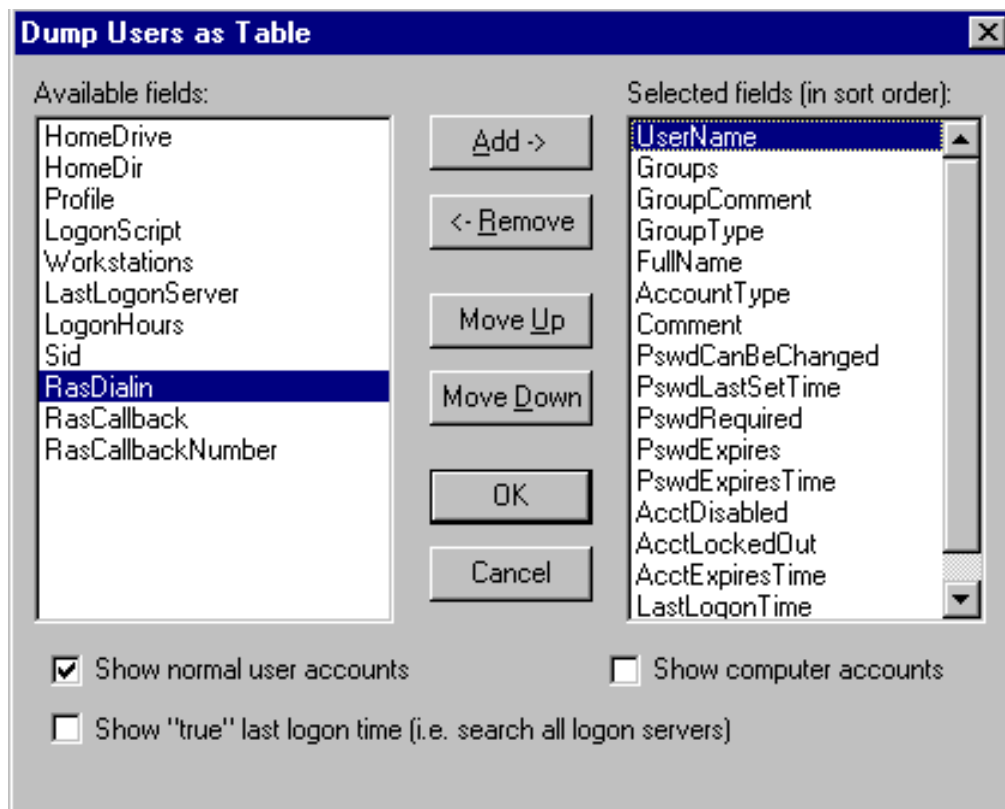
◆ DumpSec



Tools

Shareware/Freeware Utilities

◆ DumpSec



Tools

Shareware/Freeware Utilities

- ◆ DumpEvt – dump event logs (all six) for import into a database
- ◆ Pwdump2 – dumps the password hashes for cracking, whether or not SYSKEY is enabled
- ◆ LC⁵ (10phtcrack) – password auditing, supports the rainbow tables (\$)
- ◆ Rainbow Tables - Pre-computed password hash table for 99% of all possible English alphanumeric password combinations

Auditing Windows Server

What to audit?

- ◆ That depends...
- ◆ Ideal – all servers in forest/tree/domain
 - Not necessarily practical
 - Budget and time constraints

Auditing Windows Server

What to audit?

- ◆ Application audit
 - Application server(s)
 - Physical security
 - Active directory
 - Domain controller

Auditing Windows Server

What to audit?

◆ Active directory audit

- Active directory
- Domain controller(s)
- DNS servers
- Physical security
- **Trusts** (Administrative tools / Active directory domains and trusts / select domain / properties / trusts)

Auditing Windows Server

Attributes to audit

- ◆ Group Policy
 - GPM security templates
 - Pre-defined or customize
- ◆ Logon Controls
 - Password settings
 - LanMan and NTLMv1

Auditing Windows Server

Attributes to audit

◆ User Rights

- Administrators, Power Users, Backup Operators
- Manage Auditing and Security Log
- Act as part of the Operating System
- Take ownership of object

Auditing Windows Server

Attributes to audit

◆ File Permissions

- Full control
- Write
- Traverse folders
- Delete
- Take ownership

Auditing Windows Server

Attributes to audit

◆ Auditing

- Account logon
- Account management
- Policy change

◆ Monitoring controls

- Log review and issue identification and resolution

Auditing Windows Server

Attributes to audit

◆ Other

- Network
- Services
- File system (Administrative tools / Computer Management / Storage / Disk Management, check all partitions.)
- Physical Access
- User and security administration

Auditing Windows Server

Attributes to audit

- ◆ Microsoft security checklists and recommendations, see:
 - Windows Server 2003, Best Practice Guide for Securing Active Directory Installations, Version 3, Microsoft Corporation, 2003
 - Windows Server 2003 Security, Microsoft Corporation, March 2003
 - Windows Server 2003, Technical Overview of Security for Windows Server, Microsoft Corporation, July 2002
 - GPO Security Templates

Useful web sites

- ◆ <http://www.antsight.com/zsl/rainbowcrack/> - Rainbow tables
- ◆ <http://www.atstake.com/> - lophtrcrack
- ◆ <http://www.auditnet.org/>
- ◆ <http://www.bindview.com/Support/Razor/> - pwdump2
- ◆ http://www.cisecurity.org/bench_win2000.html CIS benchmark
- ◆ <http://www.foundstone.com/resources/freetools.htm> - Fport
- ◆ <http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/techref/en-us/Default.asp>
- ◆ <http://www.microsoft.com/windowsserver2003/downloads/featurepacks/default.mspx>
Group Policy Management Console
- ◆ <http://www.microsoft.com/mbsa> - MBSA
- ◆ <http://www.nii.co.in/tools.html> - DumpWin
- ◆ <http://ntsecurity.nu/> - GPList
- ◆ <http://www.shavlik.com/> - hfnetchk
- ◆ <http://www.somarsoft.com/> DumpAcl, DumpEvt

References

- ◆ Active Directory Fundamentals, TechNet, Microsoft Corporation, June 2004
- ◆ Advanced Server and Client Security, TechNet, Microsoft Corporation
- ◆ Auditing the Windows 2000 Authentication Process, Julio Silveira, July 2002
- ◆ The Definitive Guide to Windows 2000 Security, Paul Cooke
- ◆ Enforcing the “Least Privilege” Principle through Active Directory, OUs, GPOs, and Group Policy Filtering. Ricardo Rodriguez
- ◆ Managing Security with Group Policy and the Windows Server 2003 Group Policy Management Console, Norman Christopher-Knight, February 2003
- ◆ Microsoft Knowledge Base Article – 243330, Well Known Security Identifiers in Windows Server Operating Systems
- ◆ Technical Overview of Security for Windows Server 2003, TechNet, Microsoft Corporation,
- ◆ Understanding Windows® 2000 Security, Microsoft Corporation
- ◆ Windows Server 2003 Security, Microsoft Corporation, March 2003
- ◆ Windows Server 2003 Technical Reference, Microsoft Corporation