Advanced Security Measures for Clients and Servers

Wayne Harris MCSE
Senior Consultant
Certified Security Solutions

Importance of Active Directory Security

Active Directory creates a more secure network environment by requiring:
- Verification of every user’s identity
- Authorization to grant or to deny access to a resource

A breach in Active Directory security may result in:
- The loss of legitimate access to network resources
- Inappropriate disclosure or loss of sensitive information
Identifying Types of Security Threats

<table>
<thead>
<tr>
<th>Source of Threat</th>
<th>Description</th>
<th>Potential Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous Users</td>
<td>Unauthenticated access to the network as enabled membership to the Pre–Windows 2000 Compatible Access group</td>
<td>Information disclosure</td>
</tr>
<tr>
<td>Authenticated Users</td>
<td>Any user who has successfully completed the authentication process</td>
<td>Information disclosure</td>
</tr>
<tr>
<td>Service Administrators</td>
<td>Used to control directory service configuration and policies</td>
<td>Ability to launch attacks throughout the forest</td>
</tr>
<tr>
<td>Data Administrators</td>
<td>Used to add and remove organizational units (OUs), computers, users, groups and to modify Group Policy settings</td>
<td>Improper delegation may compromise administrative boundaries</td>
</tr>
<tr>
<td>Users with Physical Access to Domain Controllers</td>
<td>Any situation in which an individual can access domain controllers or administrative workstations</td>
<td>Information disclosure, data tampering, or theft</td>
</tr>
</tbody>
</table>

Establishing Secure Boundaries

<table>
<thead>
<tr>
<th>Administrative Role</th>
<th>Autonomy Means to…</th>
<th>Isolation Means to…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service administrator</td>
<td>Manage independently all or part of service administration</td>
<td>Prevent other service administrators from controlling or interfering with service administration</td>
</tr>
<tr>
<td>Data administrator</td>
<td>Manage independently all or part of the data that is stored in Active Directory or on member computers</td>
<td>Prevent other data administrators from controlling or viewing data in Active Directory or on member computers</td>
</tr>
</tbody>
</table>

**Autonomy**
- Can be achieved by delegating service or data administration

**Isolation**
- Requires that a separate forest be deployed
How to Select an Active Directory Structure

Steps:
1. Start with a single-domain forest
2. For each business unit with unique administrative requirements, determine the appropriate level of autonomy and isolation
3. Note whether the requirement pertains to delegation of service management, data management, or both
4. Determine the appropriate Active Directory structure

Securing Service Administration Accounts

- Limit the number of service administrator accounts to highly trusted personnel
- Separate administrative and user accounts for administrative users
- Hide the domain administrator account
- Never share service administration accounts
- Limit the SchemaAdmins group to temporary members
- Control the administrative logon process
Demonstration 1: Configuring Restricted Group Membership

Configure the Enterprise Admins security group as a Restricted Group

- Restrict Group Policy application to trusted individuals
- Understand the concept of taking ownership of a data object
- Reserve ownership of directory partition root objects for service administrators
- Set object ownership quotas
Protecting DNS Servers and Data

Types of attacks include:
- Modification of DNS data
- Exposure of internal IP addresses to the Internet
- Denial of service

To protect your DNS servers from these types of attacks:
- Implement Active Directory-integrated zones and use secure dynamic update
- Use separate internal and external DNS servers
- Restrict zone transfers to authorized DNS servers
- Use IPSec between DNS clients and servers
- Monitor network activity
- Close all unused firewall ports

Windows Services and Security

Windows services are applications that run on computers regardless of whether a user is logged on.

Any service or application is a potential point of attack
- Gaining control of a service will compromise system security
- Many services must be accessible from the network, which increases server vulnerability
- The solution is to run as few services on Windows services as possible

Services authentication
- All services must run in the security context of a security principal
- As a best practice, use one of the Windows Server 2003 built-in accounts as the logon accounts for Windows services
Configuring Services Using Security Templates

- Apply the Member Server Baseline security template to all member servers
- Place member servers in role-specific organizational units
- Choose a role-specific security template to enable the services required for each server role
- Use Group Policy to apply the modified template to the organizational units

Configuring Services Using the Security Configuration Wizard

- The SCW security configuration database identifies the services and ports that are required for each role or feature
- The SCW analyzes the selected server for installed roles and features to identify required services and ports
- The SCW enables you to enable or disable any additional identified or non-identified services
- The SCW configures Windows Firewall using the roles and services that you choose
- After creating the policy you can apply the policy to one or more servers, or use it to create a GPO
Determining Service Dependencies

1. Open the Services console
2. Open the Service Properties dialog box
3. Click the Dependencies tab

Demonstration 2: Configuring Services Using the Security Configuration Wizard

Use the Security Configuration Wizard to configure services and Windows Firewall

- SEA-CL1.contoso.mft
- Windows XP SP2
- Office 2003
- 10.10.0.1016

- SEA-LSA1.contoso.mft
- ISA Server 2004
- 10.10.0.1016
- 131.107.0.116

- SEA-CL1.contoso.mft
- Windows XP SP2
- Office 2003
- 131.107.0.1016

- SEA-LSA1.contoso.mft
- ISA Server 2004
- 10.10.0.1016
- 131.107.0.116

- SEA-LR1.contoso.mft
- ISA Server 2004
- 10.10.0.316
- 131.107.0.816

- SEA-LR1.contoso.mft
- ISA Server 2004
- 10.10.0.316
- 131.107.0.816
Security Auditing

- Administrators should establish an audit policy
- When establishing an audit policy:
  - Analyze the threat model
  - Consider your organization’s legal and regulatory requirements
  - Consider system and user capabilities
  - Test and refine the policy
- Separate the security auditing role from the network administration role
- Consider using centralized log monitoring tools such as:
  - Microsoft Operations Manager (MOM)
  - EventCombMT
  - Log Parser
  - SNMP

Recommended Audit Policy Settings for Member Servers

<table>
<thead>
<tr>
<th>Audit Policy</th>
<th>Recommended Minimum Settings for an Enterprise Client Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit account logon events</td>
<td>Success</td>
</tr>
<tr>
<td>Audit account management</td>
<td>Success</td>
</tr>
<tr>
<td>Audit directory service access</td>
<td>Only if required by threat model</td>
</tr>
<tr>
<td>Audit logon events</td>
<td>Success</td>
</tr>
<tr>
<td>Audit object access</td>
<td>Only if required by threat model</td>
</tr>
<tr>
<td>Audit policy change</td>
<td>Success</td>
</tr>
<tr>
<td>Audit privilege use</td>
<td>No auditing</td>
</tr>
<tr>
<td>Audit process tracking</td>
<td>Only if required by threat model</td>
</tr>
<tr>
<td>Audit system events</td>
<td>Success</td>
</tr>
</tbody>
</table>
Demonstration 3: Using EventCombMT to View Event Logs

Use EventCombMT to View Event Logs from Multiple Servers

Security Monitoring Using MOM

- MOM collects security events from managed computers or devices
- MOM analyzes collected events and raises alerts for significant events
Best Practices for Securing Servers

- Apply the latest service packs and security updates
- Limit the number of administrators and the level of administrative permissions
- Run services with a system account that has the fewest possible permissions
- Reduce the attack surface
- Use Active Directory to enforce server security
- Have an emergency response plan

Using Security Templates on Clients

Security templates can also define policy settings for securing client computers running on the Windows platform

<table>
<thead>
<tr>
<th>Security Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Policies</td>
<td>Password Policy, Account Lockout Policy, and Kerberos Policy</td>
</tr>
<tr>
<td>Local Policies</td>
<td>Audit Policy, User Rights Assignment, and Security Options</td>
</tr>
<tr>
<td>Event Log</td>
<td>Application, system, and security Event Log settings</td>
</tr>
<tr>
<td>Restricted Groups</td>
<td>Membership control of security-sensitive groups</td>
</tr>
<tr>
<td>System Services</td>
<td>Startup and permissions for system services</td>
</tr>
<tr>
<td>Registry</td>
<td>Permissions for registry keys</td>
</tr>
<tr>
<td>File System</td>
<td>Permissions for folders and files</td>
</tr>
</tbody>
</table>
Using Domain-Level Account Policies

Account policies are applied to the domain level and affect all domain accounts.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Vulnerability</th>
<th>Countermeasure</th>
<th>Potential Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Policy example: Enforce password history</td>
<td>Users reuse the same password</td>
<td>Use the maximum setting</td>
<td>Users might write down their old passwords</td>
</tr>
<tr>
<td>Account Policy example: Passwords must meet complexity requirements</td>
<td>Non-complex passwords are easy to crack</td>
<td>Enable this setting, instruct users to use pass phrases</td>
<td>Users may not remember complex passwords</td>
</tr>
<tr>
<td>Account Policy example: Minimum password age</td>
<td>Users can change passwords multiple times to enable them to reuse a password</td>
<td>Set the Minimum password age to a value of 2 days</td>
<td>If an administrator changes a user’s password, user may not be able to change it for 2 days</td>
</tr>
<tr>
<td>Kerberos Policy example: Enforce user logon restrictions</td>
<td>Users may get session tickets for unauthorized services</td>
<td>Reduce ticket validity time-out and require tighter clock synchronization</td>
<td>Increased network traffic; inability to connect to servers</td>
</tr>
</tbody>
</table>

Implementing Security Templates on Clients

- Examine the security templates in the Windows XP Security Guide v2
- Import the default templates into a GPO and modify if needed
- Deploy security templates using Group Policy objects
Securing Legacy Clients

- Windows 2000 clients can use security templates deployed through Group Policy
- Configure other clients by using scripts or policy files:
  - Use logon scripts
  - Use system policies
  - Scripts

Deployment Scenarios

<table>
<thead>
<tr>
<th>Client Computer</th>
<th>Location and Security Settings</th>
</tr>
</thead>
</table>
| Windows XP Professional (Stand-alone) | Public Internet Kiosk  
  - Implement high-security template  
  - Disallow all applications except Internet Explorer |
| Windows XP Professional (Domain Member) | Public E-mail/Application Kiosk  
  - Implement high-security template  
  - Disallow all applications except Internet Explorer and Remote Desktop |
| Windows XP and 2000 Professional (Domain Member) | Secure Business Workstation  
  - Implement enterprise client security template, and modify as required  
  - Restrict only specific applications |
| Windows XP Professional (Domain Member) | Secure Domain Management Workstation  
  - Implement high-security template, and modify as required  
  - Disallow all applications (but is not applied to administrators) |
Security Guidelines for Users

- Choose complex passwords*
- Protect passwords
- Lock unattended computers*
- Do not log on using a privileged account
- Run only trusted programs*
- Do not open suspicious attachments*
- Do not fall prey to social engineering
- Review your organization’s security policies
- Do not attempt to override security settings*
- Report suspicious incidents

*These security guidelines can be fully or partially implemented through centralized policies

Role and Limitations of File Permissions

- Intended to prevent unauthorized access
- Administrators may gain unauthorized access
- Do not protect against intruders with physical access
- Encryption provides additional security
Role and Limitations of the Encrypting File System

- **Benefit of EFS encryption**
  - Ensures privacy of information
  - Uses robust public key technology

- **Danger of encryption**
  - All access to data is lost if the private key is lost

- **Private keys on client computers**
  - Keys are encrypted with derivative of user's password
  - Private keys are only as secure as the password
  - Private keys are lost when user profile is lost

Encrypting File System Differences Between Windows Versions

- **Windows 2000 and newer Windows versions support EFS on NTFS partitions**
- **Windows XP and Windows Server 2003 include new features:**
  - Additional users can be authorized
  - Offline files can be encrypted
  - The 3DES encryption algorithm can replace DESX
  - A password-reset disk can be used
  - EFS preserves encryption over WebDAV
  - Data recovery agents are recommended
  - Usability is enhanced
Implementing Encrypting File System: How to Do It Right

- Use Group Policy to disable EFS until ready for central implementation
- Plan and design policies
- Designate recovery agents
- Assign certificates
- Implement by using Group Policy

Demonstration 4: Configuring EFS

- Configure Data Recovery Agents
- Encrypt Files
- Decrypt Files
- Share an Encrypted File
Windows Rights Management Services

- RMS protects and enhances data security for the following scenarios:
  - Protecting confidential e-mail messages
  - Enforcing document rights
  - Protecting sensitive intranet content
- It does NOT provide:
  - Unbreakable attacker-proof security
  - Protection against analog attacks

Components of Windows RMS Technology

**Server Components**
- Windows RMS for Windows Server 2003
- Software development kits (SDKs)

**Client Components**
- Windows Rights Management client software
- RMS-enabled applications
  - Microsoft Office Professional 2003
  - RM add-on for Internet Explorer
  - SDKs
How Windows RMS Works

Rights Management Service SP1 Enhancements

- Support for servers that are not connected to the Internet
- Certified against Government and Industry Standards
- Supports Smartcard-based authentication
- Provides a server lockbox
- Enhances dynamic role-based security with support for Query Based Groups in Exchange 2003
- Improved remote access while using Outlook RPC over HTTP
- Eases deployment rollout through familiar Microsoft installation technologies
Demonstration 5: Windows Rights Management Service

Using RMS to protect data

Mobile Client Security Overview

Need to secure:
- Access to the device
- Access to the stored data
- Access to the network
Group Policy Challenges for Remote Clients

- Clients might not be domain members:
  - Group Policy applies only to domain members
  - Consider a VPN with limited network access
  - Consider Network Access Quarantine Control

- Group Policy settings can be updated only when clients are connected
- Plan for slowdown if Group Policy settings are applied over slow links

Securing E-Mail Access for Remote Clients

- Native Outlook Access
- RPC over HTTP(S)
- OWA:
  - Authentication methods
  - Encryption
- POP3, IMAP, and SMTP
- OMA

Use SSL for all Internet protocols
Wireless Client Security Support

- **Windows XP:**
  - Provides native support for 802.1X

- **Windows 2000:**
  - 802.1X disabled by default
  - Configuration requires third-party utility
  - No user-specific profiles
  - Cannot use Group Policy to configure settings

Windows XP SP2 and Windows Server 2003 SP1 Wireless Client Support

- **Wireless Network Setup Wizard**
  - Used to configure and distribute wireless network settings

- **Wireless Provisioning Services (WPS)**
  - Used to automate wireless network clients configuration by creating a configuration file that is downloaded from the WPS server

- **Wireless Network (IEEE 802.11) Policies**
  - Used to configure the wireless client configuration by using Group Policy

- **Windows Server 2003 SP1 Wireless Network Policies Enhancements**
  - Extends Group Policy support to managing WPA settings for wireless clients
Best Practices for Mobile Client Users

- Protect mobile devices with passwords
- Do not store network access information on the device
- Keep the antivirus software updated
- Encrypt the data stored on the device
- Limit the data stored on the device
- Implement a regular backup procedure
- Implement policies for dealing with lost or stolen devices

Mobile Client Security Best Practices

- Require remote users to use an encrypted VPN connection
- Require multifactor authentication when feasible
- Require certificate authentication for mobile client access
- Require periodic review of audit logs
- Require strong authentication for wireless networking
Resolving Security Template Conflicts

- Use Resultant Set of Policy (RSoP) tools
  - Active Directory management tools
  - Group Policy results from the GPMC
  - GPRresult

See the Knowledge Base article, “Client, service, and program incompatibilities that may occur when you modify security settings and user rights assignments” on the Microsoft Help and Support Web site.

Troubleshooting Application Failures

- Applying security patches or security templates might prevent applications from working
- Tools for troubleshooting application failures
  - Network Monitor
  - File Monitor
  - Registry Monitor
  - Dependency Walker
  - Cipher
Troubleshooting Services and Processes

- You may need to troubleshoot services:
  1. When services and processes fail to start
  2. To confirm that all services and processes are legitimate
- Tools to troubleshoot processes:
  - Tlist.exe or Process Explorer
  - Dependency Walker
  - Examine DLL properties

Troubleshooting Network Connectivity Issues

- Ensure that only required ports are open on the computers
- Tools for determining port usage:
  - Port Reporter
  - PortQry and PortQryUI
  - TCPView
  - Netstat -o (on Windows XP or Windows Server 2003)
  - Task Manager
- Test port usage for applications and services
Best Practices for Troubleshooting

- Use a formal change and configuration management strategy
- Test all security configuration changes
- Use RSoP tools in planning mode
- Document the normal settings
- Always perform a full system backup before applying security templates
- Resolve existing problems before making more changes
- Troubleshoot securely

Session Summary

- Identify potential security threats to your Active Directory deployment
- Apply the latest security patches, limit the number of administrators, and evaluate the need for specific services
- Apply security templates to clients based upon the scenario or role of the workstations
- EFS and RMS can be used to enhance data security
- Use an encrypted VPN and multifactor authentication to secure remote user access
- Document all settings and use a formal change and configuration management strategy