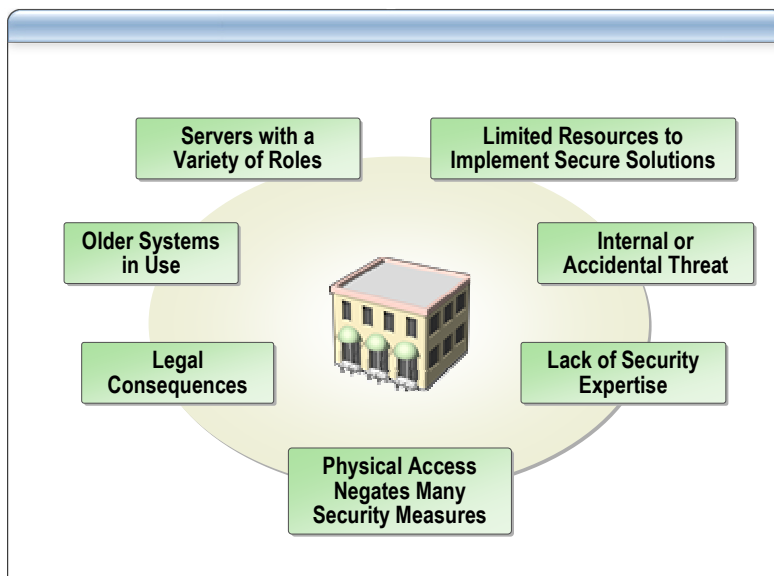


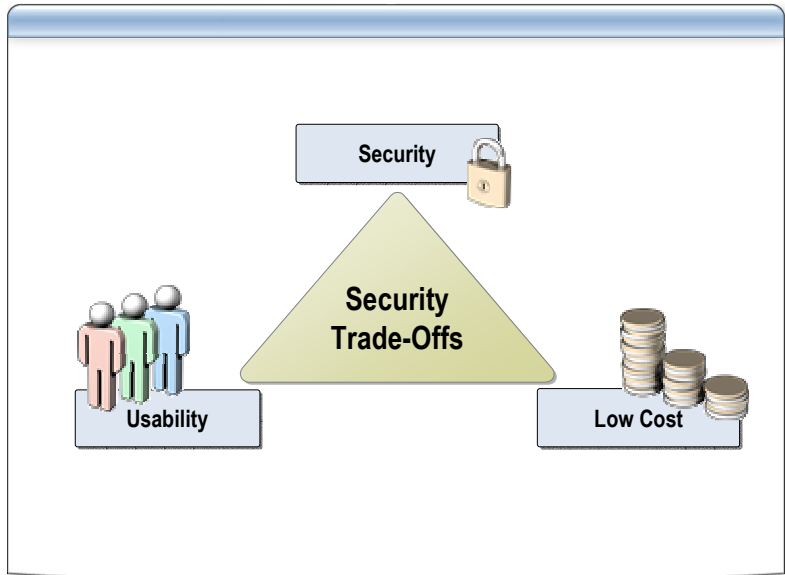
Implementing Server Security on Windows 2000 and Windows Server 2003

Wayne Harris MCSE
Senior Consultant
Certified Security Solutions

Security Challenges for Small and Medium-Sized Businesses



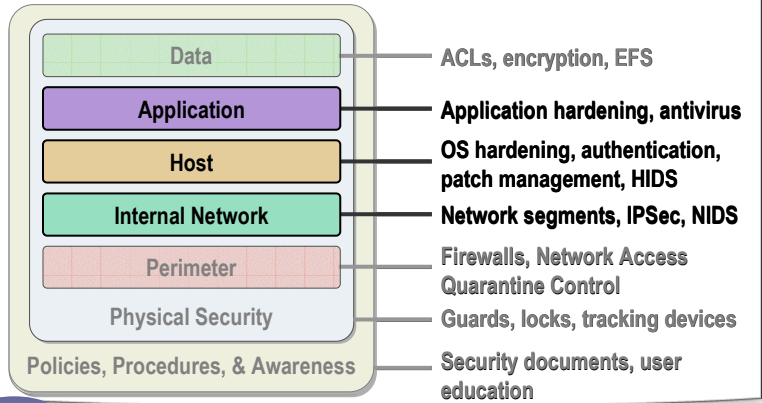
Fundamental Security Trade-Offs



Defense in Depth

Using a layered approach

- Increases an attacker's risk of detection
- Reduces an attacker's chance of success



Microsoft Windows Server Security Guidance

- *Windows 2000 Common Criteria Security Configuration Guide*
- *Windows 2000 Security Hardening Guide*
- *Securing Windows 2000 Servers*
- *Threats and Countermeasures Guide*
- *Windows Server 2003 Security Guide*

Core Server Security Practices

- Apply the latest service pack and all available security updates
- Use Group Policy to harden servers
- Use MBSA to scan server security configurations
- Restrict physical and network access to servers



Managing Software Updates

Implement an appropriate update management solution to manage software updates

Customer type	Scenario	Customer chooses
Small business	Has one to three Windows 2000 or newer servers and one IT administrator	WSUS
Medium or large enterprise	Wants an update management solution with basic level of control that updates Windows 2000 and newer versions of Windows	WSUS
	Wants a single, flexible update management solution with extended level of control to update and distribute all software	Systems Management Server

Recommendations for Hardening Servers

- ✓ Rename the built-in Administrator and Guest accounts
- ✓ Use restricted groups to limit the membership of administrative groups
- ✓ Restrict the users who can log on local on servers
- ✓ Restrict access for built-in and non operating-system service accounts
- ✓ Do not configure a service to log on using a domain account
- ✓ Use NTFS permissions to secure files and folders

Windows Server 2003 SP1 Technologies Overview

Service Pack 1 takes a proactive approach to securing the server by reducing the attack surface

- Restrict anonymous access to RPC services
- Restrict DCOM activation, launch, and call privileges and differentiate between local and remote clients
- Support for no execute hardware to prevent executables from running in memory spaces marked as nonexecutable
- VPN Quarantine
- IIS 6.0 metabase auditing



Windows Firewall

- Enabled by default in new installs
- Audit logging to track firewall activity
- Boot-time security - the firewall starts before network connections are allowed
- Global configuration - settings are applied to all network connections
- Access to open ports can be restricted based on client network
- “On with no exceptions” means that no connections are accepted
- To enable client access, add the application or service to the Windows Firewall exceptions list
- Use Group Policy or Security Configuration Wizard to manage Windows Firewall configuration

Post-Setup Security Updates

The screenshot shows the 'Windows Server Post-Setup Security Updates' wizard. At the top, it states: 'To protect your server, all inbound connections, other than those specifically opened during setup or by policy settings, are blocked until you complete the following steps.' Below this, there are two main steps:

- Step 1: Install Critical Security Updates** (with a 'More Information' link). The text explains that Microsoft continually updates Windows to help protect the server from viruses and other security threats. It notes that some updates require a restart and that users should return to Windows Update to ensure all critical updates are installed. A button labeled 'Update this server' is provided.
- Step 2: Configure Automatic Updates** (with a 'More Information' link). The text explains that the Automatic Updates feature can automatically download the latest security updates on a schedule. A button labeled 'Configure automatic updating for this server' is provided.

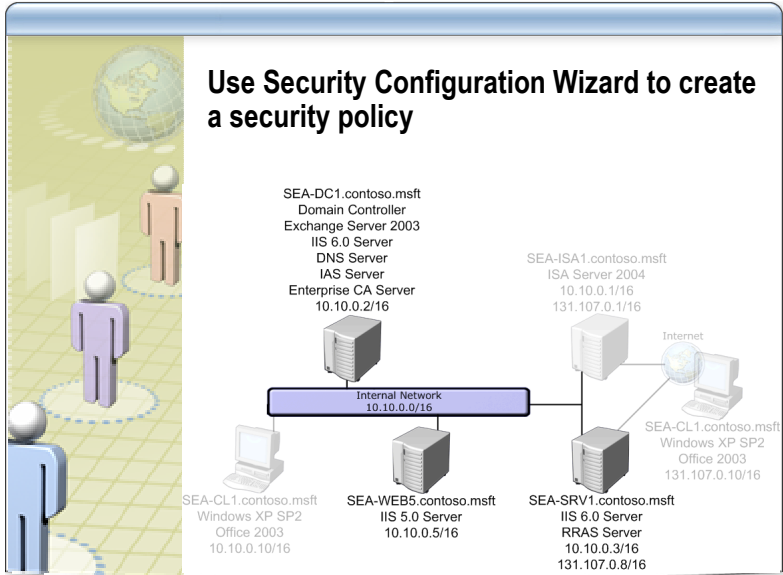
At the bottom, there is a 'Finish' button and a note: 'To close this page and allow inbound connections to this server, click Finish. For more information about blocking incoming connections, see the Security Configuration Wizard Help.'

Security Configuration Wizard

The screenshot shows the Security Configuration Wizard (SCW) overview. It is divided into two main sections:

- SCW provides guided attack surface reduction for Windows Servers**
 - Disables unnecessary services and IIS Web extensions
 - Blocks unused ports and secure ports that are left open using IPSec
 - Reduces protocol exposure (LDAP, NTLM, SMB)
 - Configures audit settings
- SCW supports:**
 - Rollback
 - Analysis
 - Remote configuration
 - Command-line support
 - Active Directory integration
 - Policy editing

Demonstration 1: Using the Security Configuration Wizard



Active Directory Components

- **Group Policy**

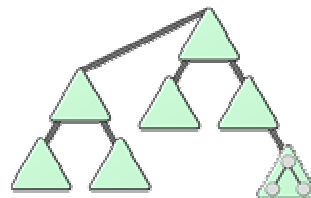
Group Policy is a key tool for implementing and managing network security

- **Forest**

A forest functions as a security boundary in Active Directory

- **Domain**

- **Organizational Unit (OU)**



Planning Active Directory Security

Analyze the environment:

- Intranet data center
- Branch office
- Extranet data center



Perform threat analysis:

- Identify threats to Active Directory
- Determine security measures for identified threats
- Establish contingency plans

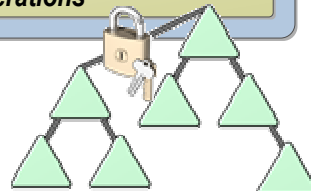


Establishing Active Directory Security Boundaries

- Specify security and administrative boundaries based on need for delegation of administration

- Design an Active Directory structure based on delegation requirements

- Implement security boundaries based on the *Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations*



Strengthening Domain Policy Settings

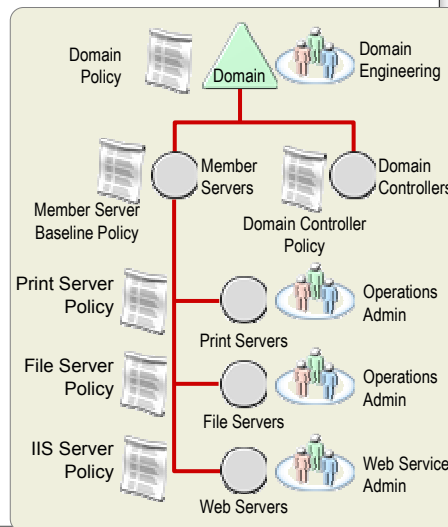
- Strengthen the settings for the Domain by creating and linking a new GPO at the domain level
- Ensure that password and account policies meet your organization's security requirements
- Analyze threats and update security policy to reflect and counter those threats



Establishing a Role-Based OU Hierarchy

An OU hierarchy based on server roles:




- Simplifies security management issues
- Applies security policy settings to servers and other objects in each OU



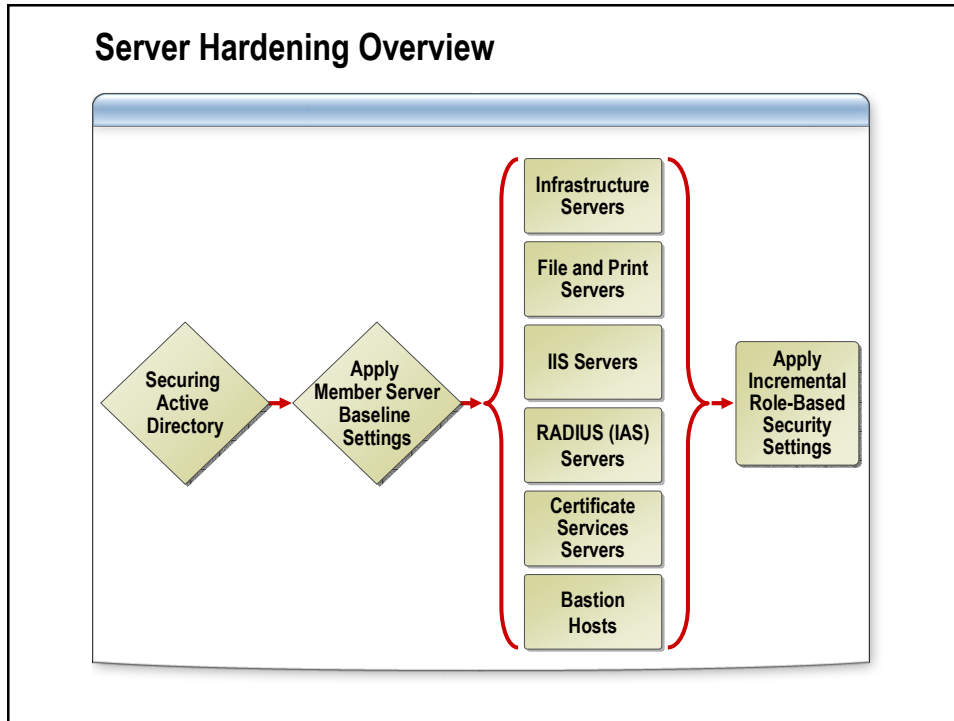
How to Create an OU Hierarchy for Managing and Securing Servers

- 1** Create an OU named Member Servers
- 2** Create OUs within the Member Servers OU for each server role
- 3** Move each server object into the appropriate OU according to role
- 4** Delegate control of each role-based OU to the appropriate security group
- 5** Assign security templates using GPOs linked to the appropriate OUs

Administrative Best Practices

-  Distinguish between service and data administrative roles
-  Take steps to secure administrative accounts
-  Delegate the minimum permissions required





Member Server Baseline Security Template




Modify and apply the Member Server Baseline security template to all member servers

Settings in the Member Server Baseline security template:

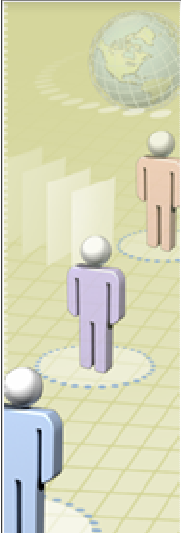
- Audit Policy
- User Rights Assignment
- Security Options
- Event Log
- System Services

The diagram shows a server rack and a padlock icon, symbolizing security.

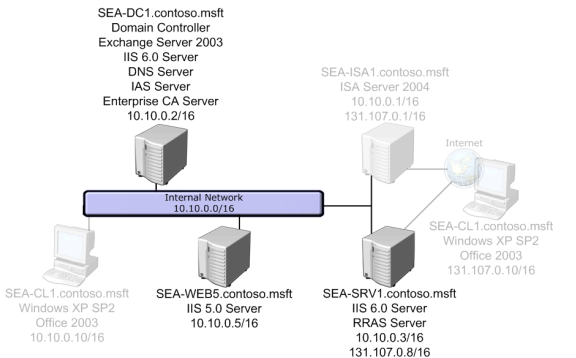
Security Template Types

Template type	Security level/Environment
Legacy Client	<ul style="list-style-type: none"> Provides adequate security Used where Active Directory is used with Windows 98 clients or with Windows NT 4.0 clients and member servers 
Enterprise Client	<ul style="list-style-type: none"> Provides solid security Used where Active Directory is used with Windows 2000 or later clients and servers 
High Security	<ul style="list-style-type: none"> Provides very strong security Used only where security is the preeminent concern, and Active Directory is used with Windows 2000 or later clients and servers 

Demonstration 2: Creating an OU Structure and Applying a Security Template



- View and modify the Member Server Baseline security template
- Create an OU structure to facilitate Group Policy
- Create a GPO for the Member Servers OU, and import a security template into the GPO
- Verify that the GPO has been applied



```

graph TD
    subgraph Internal_Network [Internal Network 10.10.0.0/16]
        SEA-DC1[SEA-DC1.contoso.msft  
Domain Controller  
Exchange Server 2003  
IIS 6.0 Server  
DNS Server  
IAS Server  
Enterprise CA Server  
10.10.0.2/16]
        SEA-CL1[SEA-CL1.contoso.msft  
Windows XP SP2  
Office 2003  
10.10.0.10/16]
        SEA-WEB5[SEA-WEB5.contoso.msft  
IIS 5.0 Server  
10.10.0.5/16]
        SEA-SRV1[SEA-SRV1.contoso.msft  
IIS 6.0 Server  
RRAS Server  
10.10.0.3/16  
131.107.0.8/16]
    end
    SEA-DC1 --- SEA-CL1
    SEA-DC1 --- SEA-WEB5
    SEA-DC1 --- SEA-SRV1
    SEA-SRV1 --- Internet
    SEA-ISA1[SEA-ISA1.contoso.msft  
ISA Server 2004  
10.10.0.1/16  
131.107.0.1/16] --- Internet
    SEA-ISA1 --- SEA-SRV1
    
```

Best Practices for Using Security Templates

- ✓ Review and modify security templates before using them
- ✓ Use Security Configuration and Analysis tool to review template settings before applying them
- ✓ Test templates thoroughly before deploying them
- ✓ Store security templates in a secure location
- ✓ Audit all modifications to Group Policy objects

Using the Security Configuration Wizard and Security Templates

You can use security templates or SCW or both to configure server security

- Security templates provide security configuration based on generic roles that can be deployed to servers and clients using GPOs
- SCW provides more specific security configurations for servers performing a specific role or combination of roles
- SCW policies can be converted into GPOs by using the scwcmd transform command
- Use caution when combining the use of security templates and SCW policies

Security Threats to Domain Controllers

- Modification of Active Directory data
- Password attacks against administrator accounts
- Denial-of-service attacks
- Replication prevention attacks
- Exploitation of known vulnerabilities

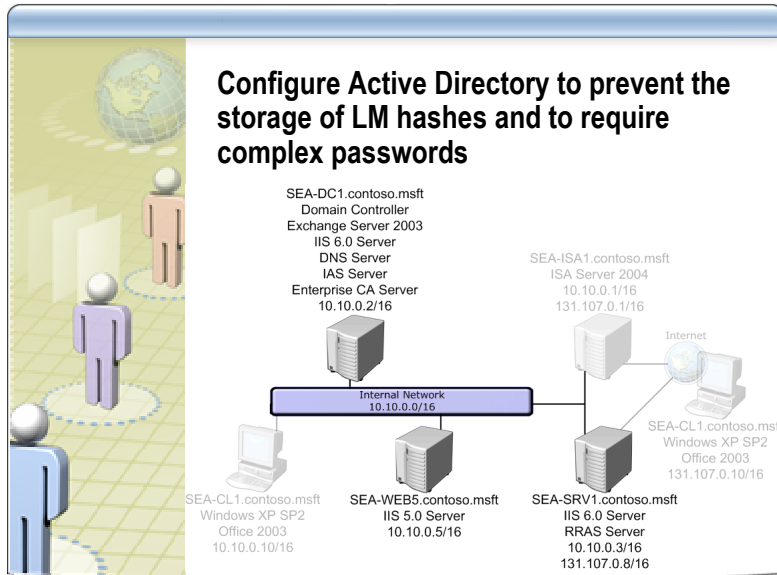


Implement Password Security

- Do not implement authentication protocols that require reversible encryption
- Disable LM hash value storage in Active Directory
- Require complex passwords for all user accounts



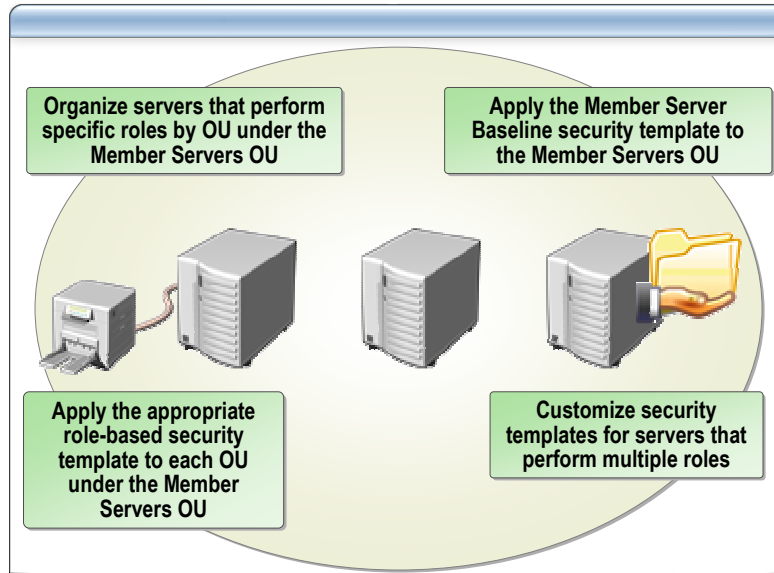
Demonstration 3: Configuring Password Security



Best Practices for Hardening Domain Controllers

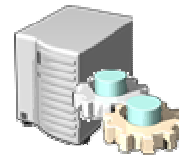
- ✓ **Physically secure domain controllers**
- ✓ **Use Group Policy to apply the Domain Controller security template to all domain controllers**
- ✓ **Disable services that are not required**
- ✓ **Do not run services on domain controllers using the same accounts used to run services on other computers**
- ✓ **Implement appropriate auditing and event log settings**
- ✓ **Install at least two domain controllers in each domain**

Using Security Templates for Specific Server Roles



Hardening Infrastructure Servers

- Apply the Infrastructure Server security template
- Manually configure additional settings as appropriate:
 - Configure DHCP logging
 - Protect against DHCP DoS attacks
 - Use Active Directory integrated DNS zones
 - Use IPSec filters to restrict ports



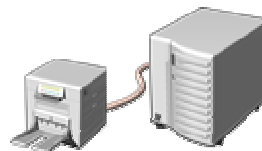
Hardening File Servers

- Apply the security settings in the File Server security template
- Manually configure additional settings on each file server:
 - Disable DFS and FRS if not required
 - Secure all shared files and folders by using NTFS and share permissions
 - Enable auditing of critical files
 - Restrict ports by using IPsec filters



Hardening Print Servers

- Apply the security settings in the Print Server security template
- Manually configure additional settings on each print server:
 - Ensure that the Print Spooler service is enabled
 - Ensure that SMB signing is not required by the print server
 - Restrict ports by using IPsec filters



Hardening IIS Servers (Part 1)

- Apply the security settings in the IIS Server security template
- If possible, upgrade Web servers to Windows Server 2003 and IIS 6.0
- Install and run the IIS Lockdown Wizard and configure URLScan to help secure IIS 4.x and 5.x installations

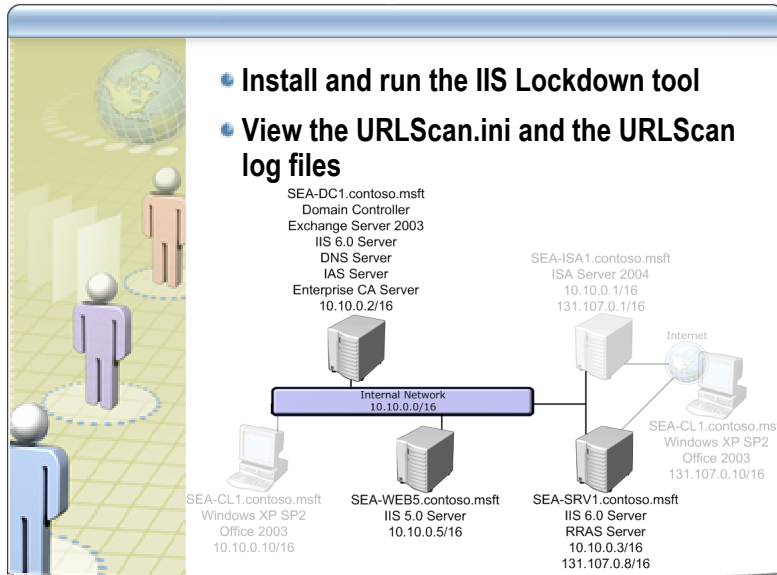


Hardening IIS Servers (Part 2)

- **Manually configure each IIS server:**
 - Enable only essential IIS components
 - Install IIS and store Web content on a dedicated disk volume
 - Configure NTFS permissions for all folders that contain Web content
 - Do not enable both the Execute and Write permissions on the same Web site
 - On IIS 5.0 servers, run applications using Medium or High Application Protection
 - Use IPSec filters to allow only TCP Port 80 and Port 443



Demonstration 4: Hardening IIS 5.0 Servers



Hardening IIS 6.0 Servers with Security Configuration Manager

When you run SCW on an IIS 6.0 server, you can configure the following settings:

- Server roles
- Disable services
- Enable Windows Firewall and enable port filtering
- Configure authentication methods
- Configure audit policy
- Enable or disable Web Service Extensions
- Remove legacy virtual directories
- Block anonymous write access

Best Practices for Hardening Servers for Specific Roles

- ✓ Modify security templates as needed for servers with multiple roles
- ✓ Enable only services required by role
- ✓ Enable service logging to capture relevant information
- ✓ Use IPSec filtering to block all ports except the specific ports needed, based on server role
- ✓ Secure service accounts and well-known user accounts

Applying Security Templates on Stand-Alone Servers

- You must manually apply security settings to each stand-alone server
- You may need to create a customized security template for each stand-alone server
- Use the Security Configuration and Analysis tool, Secedit, or GPEdit.msc to apply security template settings on stand-alone servers



Using the Security Configuration Wizard on Stand-Alone Servers

- Use the SCW to create a security policy, and apply the policy to servers with the same role
- Use the SCW command line options to manage SCW security policies
- Use a machine list file to analyze or configure multiple servers



Best Practices for Hardening Stand-Alone Servers

- ✓ Create a customized security template for each type of stand-alone server
- ✓ Enable only services required by role
- ✓ Enable service logging to capture relevant information
- ✓ Use IPSec filters to restrict ports based on server role
- ✓ Consider using SCW rather than security templates for specific server roles

Session Summary

- ✓ Implement a defense-in-depth approach to security
- ✓ Consider deploying Windows Server 2003 SP1
- ✓ Domain administrators must be highly trusted and follow secure practices
- ✓ Design your OU structure and GPOs to deploy security templates based on server roles
- ✓ Require complex passwords and store passwords securely
- ✓ Use incremental security templates for servers with specific roles
- ✓ Consider using SCW for specific server roles

Next Steps

- Find additional security training events on the Microsoft Events and Webcasts Web site
- Sign up for security communications on the Microsoft Technet Web site
- Order the Security Guidance Kit from the Microsoft Technet Security Center
- Get additional security tools and content from the Microsoft Security Center Web site