

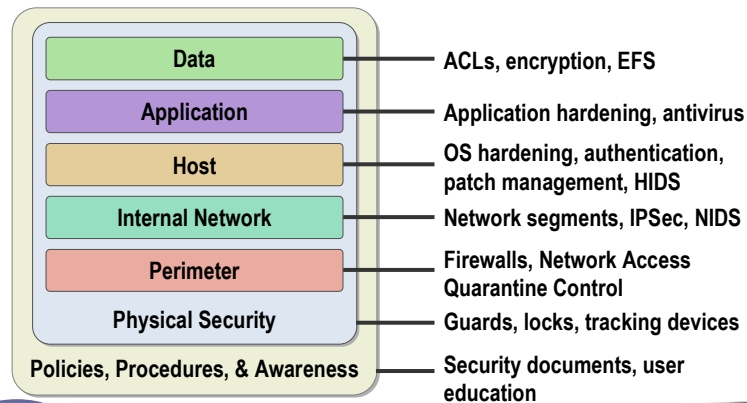
# Implementing Application Security

Wayne Harris MCSE  
Senior Consultant  
Certified Security Solutions

## Defense-in-Depth

Using a layered approach

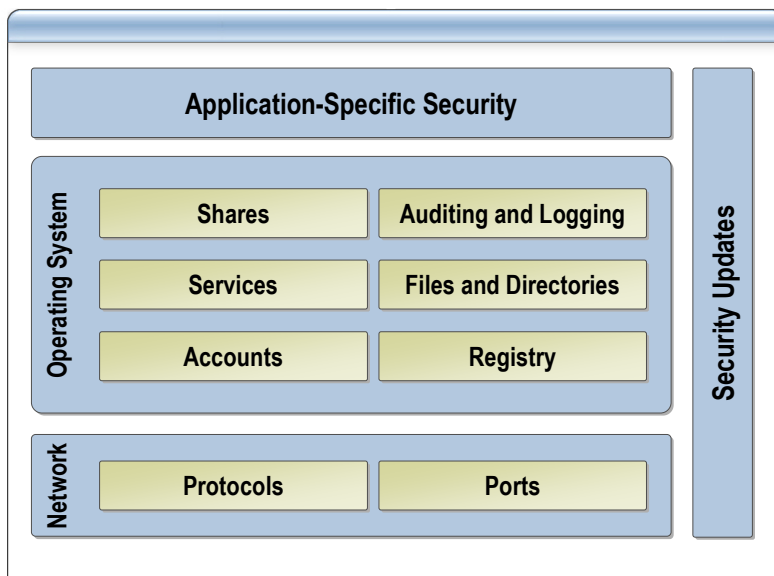
- Increases an attacker's risk of detection
- Reduces an attacker's chance of success



### Why Application Security Matters

- Perimeter defenses provide limited protection
- Most host-based defenses are not application-specific
- Most modern attacks occur at the application layer

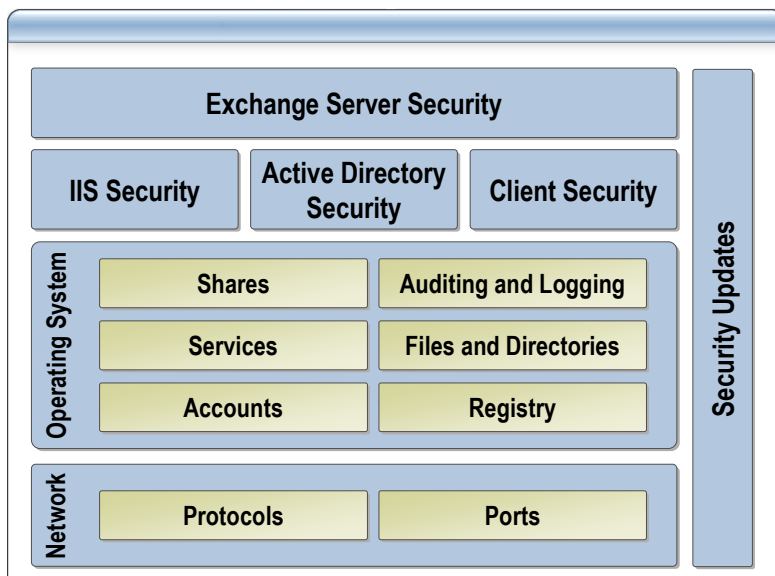
### Application Security Dependencies



### Application Server Best Practices

- ✓ Configure security on the base operating system
- ✓ Apply operating system and application service packs and updates
- ✓ Install or enable only those services and applications that are required
- ✓ Assign only those permissions needed to perform required tasks
- ✓ Application service accounts should be configured with minimal permissions
- ✓ Apply defense-in-depth principles to increase protection

### Exchange Server Security Dependencies



## Aspects of Exchange Server Security

- **Securing the Exchange Server computer**
- **Securing access to Exchange Server**
  - Blocking unauthorized access
- **Securing communications**
  - Blocking and encrypting communications
- **Blocking spam**
  - Filtering incoming mail
  - Relay restrictions: Don't aid spammers!
- **Blocking insecure e-mail messages**
  - Virus scanning
  - Attachment blocking

## Securing Exchange Servers Using Security Templates

- **Exchange 2000 Server Back-End Servers**
  - Apply baseline security template and the Exchange back-end incremental template
- **Exchange 2000 Server Front-End Servers**
  - Apply baseline security template and the Exchange front-end incremental template
- **Exchange 2000 Server OWA Server**
  - Apply IIS Lockdown, including URLScan
- **Exchange Server 2003 Back-End**
  - Apply protocol security templates
- **Exchange Server 2003 Front-End and OWA Server**
  - IIS 6.0 provides much of the same functionality as URLScan and IISLockdown
- **Domain Controllers with Exchange Server**
  - Apply the domain controller baseline template (BaselineDC.inf), and then apply the Exchange DC incremental template

## Securing Exchange Servers Using Security Configuration Wizard

- SCW is an additional component with Windows Server 2003 SP1
- SCW provides guided attack surface reduction for servers running Windows that:
  - Configures servers based on roles
  - Disables unnecessary services
  - Disables unnecessary IIS Web extensions
  - Blocks ports that are not required
- Run SCW on an Exchange server in a specific role, then import the settings on other servers in the same role
- To apply SCW settings using GPOs, use the Scwcmd Transform command to create a GPO

## Securing Client Authentication

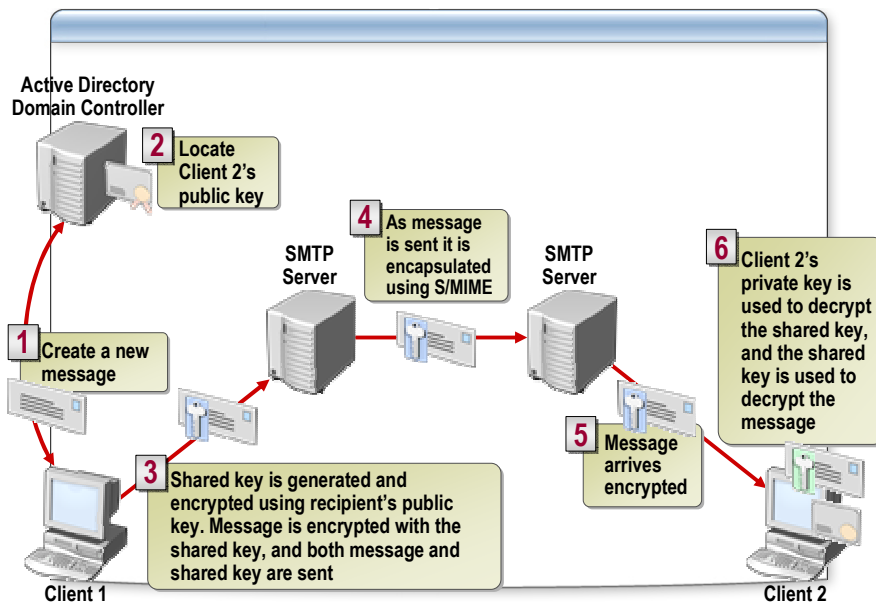
- Secure Outlook client authentication
- Configure Exchange and Outlook 2003 to use RPC over HTTPS
- Use SPA and SSL to encrypt authentication and messages for Internet protocol clients
- OWA supports several authentication methods:

Authentication Method	Considerations
Basic authentication	• Broad client support, but must use SSL for encryption
Integrated Windows authentication	• Limited client support; issues across firewalls
Digest authentication	• Limited client support
Forms-based authentication	• Cookie-based authentication method available with Exchange Server 2003

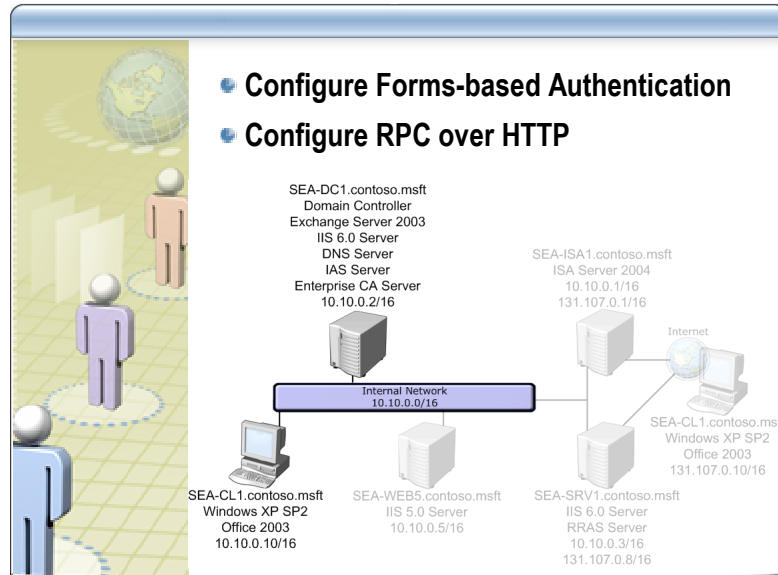
## Securing Client Communication

- **Configure RPC encryption**
  - Client-side setting
  - Can be enforced with ISA Server 2004
- **Use RPC over HTTPS for remote Outlook 2003 clients**
- **Use firewalls like ISA Server to enable secure remote client connections to Exchange Server**
- **Require SSL for OWA client connections**
- **Use S/MIME for message encryption**

## Encrypting Messages by Using S/MIME



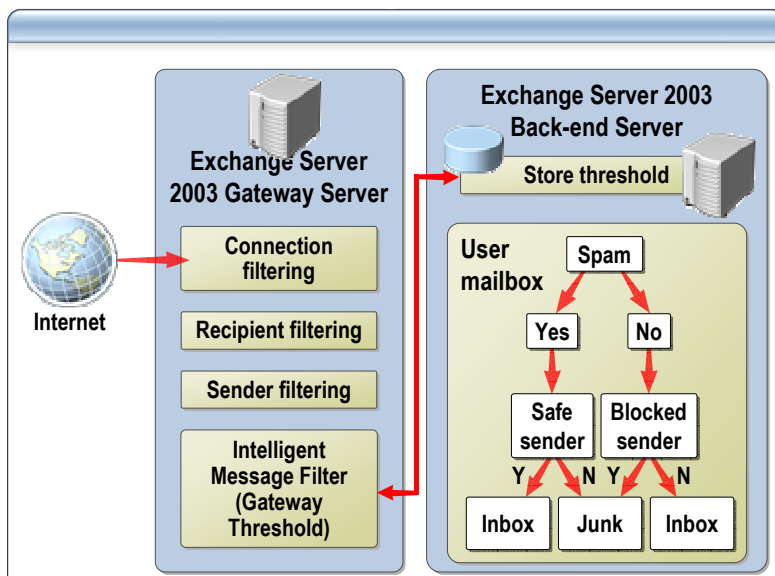
## Demonstration 1: Securing Exchange Client Communication



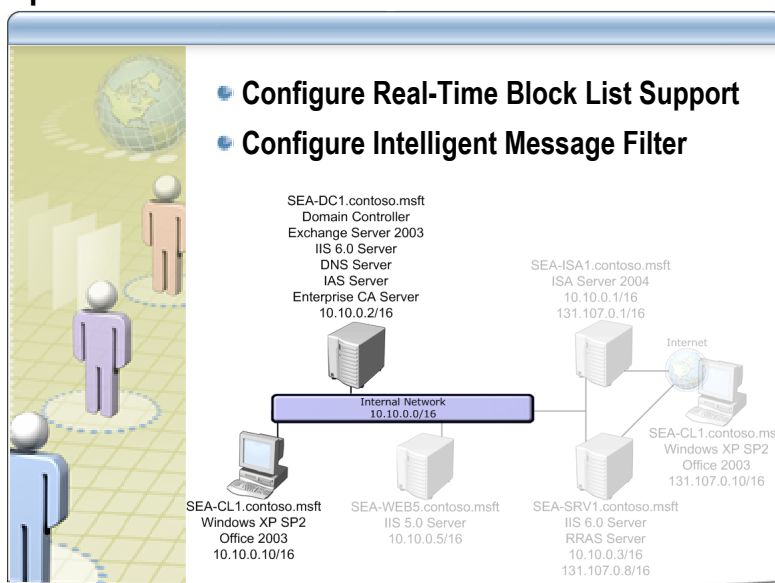
## Blocking Spam with Exchange Server 2003

- Use anti-spam features in Exchange Server 2003
  - Support for real-time block lists
  - Global deny and accept lists
  - Sender and inbound recipient filtering
  - Improved anti-relaying protection
  - Integration with Outlook 2003 and third-party anti-spam products

### Blocking Spam with Intelligent Message Filter



### Demonstration 2: Configuring Exchange Server Spam Protection



## Protecting Against E-mail Viruses

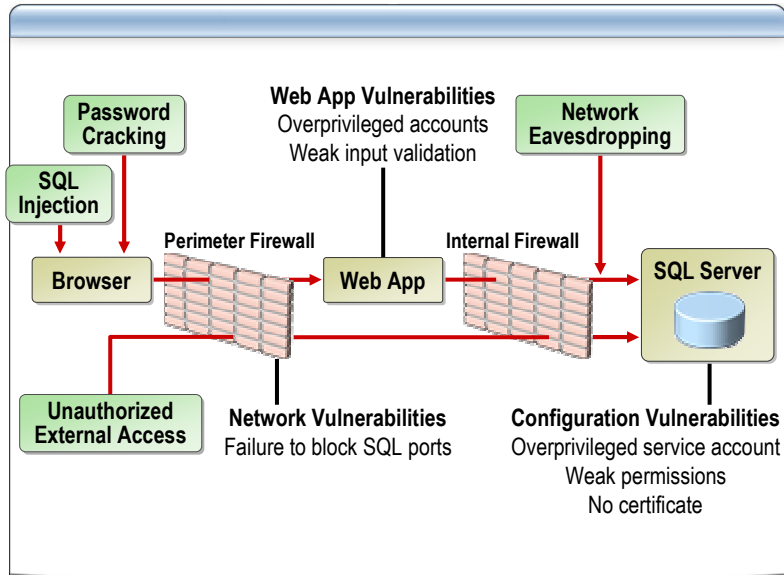
- **Implement a defense-in-depth approach**
  - Install an anti virus scanner on the SMTP gateway server
  - Install anti virus software on the Exchange servers
  - Install anti virus software on all clients
- **Ensure that the anti virus software is compatible with Exchange Server**
- **Configure Outlook and OWA attachment security**

## Top 10 Actions to Secure Exchange Server

- 1 Install the latest service packs
- 2 Install applicable security updates
- 3 Apply the principle of least privilege
- 4 Harden the Exchange servers
- 5 Secure the e-mail clients
- 6 Use a layered antivirus approach
- 7 Implement anti-spam measures
- 8 Use an application-layer firewall such as ISA Server
- 9 Secure Outlook Web Access
- 10 Implement a backup strategy

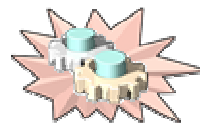
Use Exchange Best Practices Analyzer to examine the Exchange Server organization based on Microsoft best practices

### Common Database Server Threats

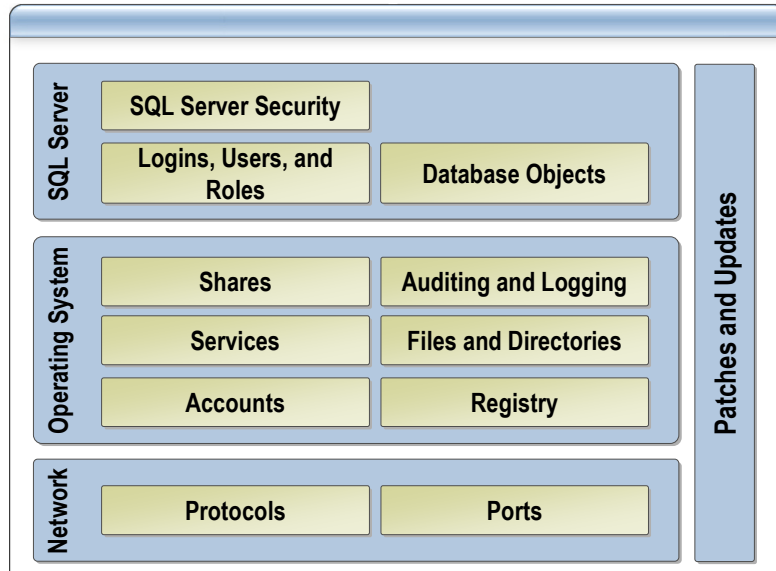


### Basic Security Configuration

- Follow a defense-in-depth approach to securing SQL Server
- Apply service packs and patches
  - Use MBSA to detect missing SQL updates
- Disable unused services
  - MSSQLSERVER (required)
  - SQLSERVERAGENT
  - MSSQLServerADHelper
  - Microsoft Search
  - Microsoft DTC



## Database Server Security Categories



## Network Security

- **Restrict SQL to TCP/IP**
  - Control who can connect to the server via IPSec policy
  - Enforce Kerberos authentication
- **Harden the TCP/IP stack**
- **Restrict ports**
  - Block all ports with the exception of the SQL Server port and ports required for authentication
  - Configure IPSec to restrict access to ports 1433 and 1434

## Operating System Security

- **Configure the SQL Server service account with the lowest possible permissions**
  - Service account should not be granted permissions to the Administrators or Users group
- **Delete or disable unused accounts**
  - Can be a haven for an attacker who has gained access
  - Audit local accounts/delete those that are not required
- **Secure authentication traffic**
  - Configure Windows to require NTLM v2

## Logins, Users, and Roles

- **Use a strong system administrator (sa) password**
- **Remove the SQL Server guest user account**
- **Remove the BUILTIN\Administrators server login**
- **Do not grant permissions for the public role**

## Files, Directories, and Shares

### • Verify permissions:

- On SQL Server installation directories
  - To ensure that the Everyone group does not have permissions to SQL Server files
  - To ensure that Registry keys are configured with proper ACLs
  - On required shared folders and remove unnecessary shares
- **Remove passwords that may exist in log files (use KillPwd.exe)**
- **Secure or remove tools, utilities, and SDKs**

## SQL Server Authentication Best Practices

### Set authentication to Windows only

- Credentials are not passed over the network
- Security is easier to manage
- Credentials delegation is available
- Eliminates the need to store passwords on clients



## SQL Server Auditing

- Log all failed Windows logon attempts
- Log successful and failed actions across the file system
- Enable SQL Server logon auditing
- Enable SQL Server general auditing



## Securing Database Objects

- Remove the sample databases
- Restrict access to stored procedures
  - Create SQL logon
  - Map logon to database user
  - Add database user to user-defined database role, then grant permissions to database role
- Restrict cmdExec access to the Sysadmin role

## Using Views and Stored Procedures

- **SQL queries may contain confidential information**
  - Names of database components
  - Server names
  - Processing logic
  - Account names or passwords
- **Use stored procedures whenever possible**
- **Use views instead of direct table access**
- **Implement security best practices for Web-based applications**

## Securing Web Applications

- **Validate all data input**
- **Secure authentication and authorization**
- **Secure sensitive data**
- **Use least-privileged process and service accounts**
- **Configure auditing and logging**
- **Use structured exception handling**

## SQL Server and Windows Server 2003 SP1

- **Windows Firewall enabled by default on slipstreamed installations**
  - No TCP/UDP/Multi-Protocol/Named Pipes port listening is enabled by default for any SQL Server component
  - Shared memory is unaffected; connections on the same machine continue to work against SQL Server/MSDE
- **Getting SQL Server back on the network**
  - Create an exception for each instance of SQL Server within Windows Firewall
  - Create an exception for each SQL Server component
  - Define connectivity-specific port that will be used for each SQL Server component and each instance of SQL Server

## SQL Server 2005 Security Features

- **Computing Initiative SQL Server 2005 development is based on the processes defined by the Trustworthy**
  - Secure by design - data encryption in the database, multiple proxy accounts, SQL Profiler does not need administrator rights
  - Secure by default – only required services are installed and started, enforced passwords for standard logon
  - Secure in deployment – granular permissions controlled by policies, separation of users and schema
  - Secure communications – Kerberos authentication for clusters, encrypted communication for Analysis server

## Top 10 Actions to Protect SQL Server

- 1 Install the most recent service pack
- 2 Run MBSA and update identified security issues
- 3 Configure Windows authentication
- 4 Isolate the database servers
- 5 Check the sa password, and ensure that it is complex
- 6 Limit privileges of SQL Server services
- 7 Block ports at your firewall
- 8 Use NTFS
- 9 Remove setup files and sample databases
- 10 Audit connections

Use SQL Server Best Practices Analyzer to examine the SQL Server configuration based on Microsoft best practices

## IIS Lockdown Tool

- The IIS Lockdown Tool turns off unnecessary features to reduce the attack surface of IIS 4.0, IIS 5.0, and IIS 5.1
- To provide defense-in-depth, the Lockdown Tool integrates URLScan, which includes customized templates for each supported server role
- IIS 6.0 is installed with Security Settings configured in previous versions of IIS Lockdown, therefore no IIS Lockdown for IIS 6.0



## URLScan

- URLScan helps prevent potentially harmful requests from reaching the server
- URLScan restricts the types of HTTP requests that IIS will process:
  - Requests for long URLs
  - Requests using alternate character sets
  - Requests containing disallowed methods
  - Requests matching any pattern
- IIS 6.0 implements most of the URLScan functions so URL scan is only required to enable customized content blocking

## Top 10 Actions to Secure IIS 5.x

- 1 Harden the operating system and apply all relevant security updates
- 2 Remove unnecessary components
- 3 Run the IIS Lockdown Tool
- 4 Configure URLScan
- 5 Place content on a separate NTFS partition
- 6 Protect files by using minimal permissions
- 7 Require encryption for sensitive Web traffic
- 8 Do not enable both the Execute and Write permissions on the same Web site
- 9 Run applications using Medium or High application protection
- 10 Use IPSec filtering to allow only required traffic (HTTP and HTTPS) to the Web server

## Security Enhancements in IIS 6.0

IIS 6.0 is locked down with the strongest time-outs and content limits set by default

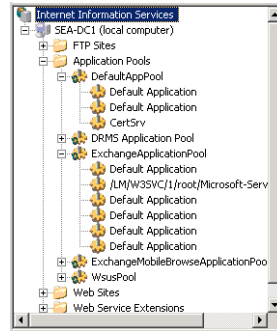
Feature	Description
<b>Locked-down server</b>	IIS 6.0 is not installed by default. A clean install only provides static file support
<b>Web service extensions list</b>	The default installation does not compile, execute, or serve files with dynamic content
<b>Default low-privilege account</b>	IIS processes run with significantly lowered privileges by logging on using the NETWORK SERVICE account
<b>Authorization</b>	URL authentication with Authorization Manager. Constrained, delegated authentication
<b>URL checking</b>	Configure time-outs and URL length limits. Checking whether file exists before attempting to run it. No executable virtual directories
<b>Process isolation</b>	Improved sandboxing of application. Third-party code runs only in worker processes, resource recycling

## Securing IIS 6.0 Using Security Configuration Wizard

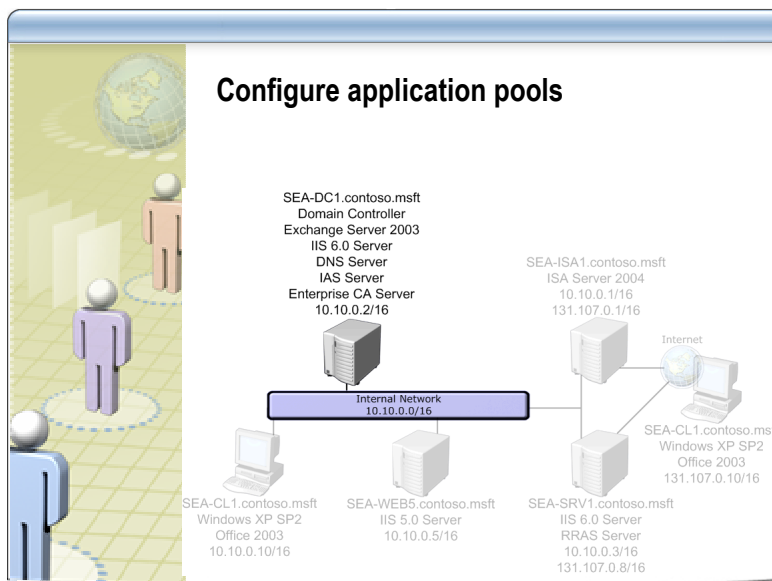
- **When you run SCW on an IIS 6.0 server, you can configure the following settings:**
  - Server roles
  - Disable services
  - Enable Windows Firewall and enable port filtering
  - Configure authentication methods
  - Configure audit policy
  - Enable or disable Web Service Extensions
  - Remove legacy virtual directories
  - Block anonymous write access

## IIS 6.0 Application Pools

- Application pools are isolated sets of applications and the worker processes that service them
- If an application fails, it does not affect the availability of applications that are running in other application pools
- Create separate application pools for applications that do not depend on each other



## Demonstration 3: Securing IIS 6.0



## Windows Small Business Server Overview

- **Windows Small Business Server 2003 provides a complete server solution for small businesses including:**
  - Providing e-mail, networking, and Internet connectivity
  - Enabling Small Business Intranet with Microsoft Windows SharePoint Services
  - Enabling remote access
  - Enabling mobile user access
  - Simplified server administration and management

## Windows Small Business Server Security

- **Security Issues for Small Business**
  - Lack of security expertise
  - Limited resources for isolating services
  - Limited security monitoring capability
  - Improper use of server resources
- **Windows Small Business Server Security Risks**
  - Many services installed by default
  - Direct connectivity to the Internet


## Protecting Against External Threats

- **Configure password policies to require complex passwords**
- **Configure secure remote access**
  - Remote Web Workplace
  - Remote Access
- **Disable all remote access options that you do not require**
- **Rename the Administrator account**
- **Implement Exchange Server and IIS security best practices**
- **Install only required software on the server**

## Protecting Against Internal Threats


- **Implement an antivirus solution**
- **Implement a backup plan**
- **Run MBSA to check for security vulnerabilities**
- **Control access permissions**
- **Educate users**
- **Do not use the server as a workstation**
- **Physically secure the server**
- **Update the software**


## Session Summary

 Secure the base operating system on all application servers

 Secure clients and client connections to Exchange Server

 Secure SQL Server authentication and database permissions

 Implement IIS 6.0 to take advantage of its security enhancements

 Enable only required services in Windows Small Business Server