Microsoft® Official Course

Module 12
Securing Windows Servers Using Group Policy Objects
Module Overview

- Windows Operating Systems Security Overview
- Configuring Security Settings
- Restricting Software
- Configuring Windows Firewall with Advanced Security
Lesson 1: Windows Operating Systems Security Overview

- Discussion: Identifying Security Risks and Costs
- Applying Defense-In-Depth to Increase Security
- Best Practices for Increasing Security
Discussion: Identifying Security Risks and Costs

• What are some of security risks in Windows-based networks?
Applying Defense-In-Depth to Increase Security

Defense-in-depth uses a layered approach to security
• Reduces an attacker’s chance of success
• Increases an attacker’s risk of detection

<table>
<thead>
<tr>
<th>Policies, procedures, and awareness</th>
<th>Security documents, user education</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical security</td>
<td>Guards, locks, tracking devices</td>
</tr>
<tr>
<td>Perimeter</td>
<td>Firewalls, network access quarantine control</td>
</tr>
<tr>
<td>Networks</td>
<td>Network segments, IPsec, Forefront TMG 2010</td>
</tr>
<tr>
<td>Host</td>
<td>Hardening, authentication, update management</td>
</tr>
<tr>
<td>Application</td>
<td>Application hardening, antivirus</td>
</tr>
<tr>
<td>Data</td>
<td>ACLs, EFS, BitLocker, backup/restore procedures</td>
</tr>
</tbody>
</table>
Best Practices for Increasing Security

Some best practices for increasing security are:
• Apply all available security updates quickly
• Follow the principle of least privilege
• Use separate administrative accounts
• Restrict administrator console sign-in
• Restrict physical access
Lesson 2: Configuring Security Settings

- Configuring Security Templates
- Configuring User Rights
- Configuring Security Options
- Configuring User Account Control
- Configuring Security Auditing
- Configuring Restricted Groups
- Configuring Account Policy Settings
- What Is Security Compliance Manager?
Configuring Security Templates

Security Templates categories:
• Account Policies
• Local Policies
• Event Log
• Restricted Groups
• System Services
• Registry
• File System

How Security Templates are distributed:
• Secedit.exe
• Security Templates Snap-in
• Security Configuration and Analysis Wizard
• Group Policy
• Security Compliance Manager (SCM)
Configuring User Rights

User Rights Types:
• Privileges
• Logon Rights

Examples of common user rights:
• Add workstations to domain
• Allow log on locally
• Allow log on through Remote Desktop Services
• Back up files and directories
• Change the system time
• Force shutdown from a remote computer
• Shut down the system
Configuring Security Options

**Security options settings:**
- Administrator and Guest account names
- Access to CD/DVD drives
- Digital data signatures
- Driver installation behavior
- Logon prompts
- User Account Control

**Examples:**
- Prompt user to change password before expiration
- Do not display last user name
- Rename administrator account
- Restrict CD-ROM access to locally logged-on users only
Configuring User Account Control

- UAC is a security feature that prompts the user for an administrative user’s credentials if the task requires administrative permissions.
- UAC enables users to perform common daily tasks as non-administrators.
Configuring Security Auditing

When using security auditing to log security-related events, you can:

- Configure security auditing according to your company’s security regulations
- Filter the Security Event Log in Event Viewer to find specific security related events
Group Policy can control group membership:

• For any group on a domain-joined computer, by applying a Group Policy Object (GPO) to the Organizational Unit (OU) containing the computer account

• For any group in AD DS, by applying a GPO to the Domain Controller’s OU
## Configuring Account Policy Settings

Account policies mitigate the threat of brute force guessing of account passwords.

<table>
<thead>
<tr>
<th>Policies</th>
<th>Default settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
<td>• Controls complexity and lifetime of passwords</td>
</tr>
<tr>
<td></td>
<td>• Max password age: 42 days</td>
</tr>
<tr>
<td></td>
<td>• Min password age: 1 day</td>
</tr>
<tr>
<td></td>
<td>• Min password length: 7 characters</td>
</tr>
<tr>
<td></td>
<td>• Complex Password: enabled</td>
</tr>
<tr>
<td></td>
<td>• Store password using reversible encryption: disabled</td>
</tr>
<tr>
<td><strong>Account lockout</strong></td>
<td>• Controls how many incorrect attempts can be made</td>
</tr>
<tr>
<td></td>
<td>• Lockout duration: not defined</td>
</tr>
<tr>
<td></td>
<td>• Lockout threshold: 0 invalid logon attempts</td>
</tr>
<tr>
<td></td>
<td>• Reset account lockout after: not defined</td>
</tr>
<tr>
<td><strong>Kerberos</strong></td>
<td>• Subset of the attributes of domain security policy</td>
</tr>
<tr>
<td></td>
<td>• Can only be applied at the domain level</td>
</tr>
</tbody>
</table>
SCM is a free tool from Microsoft that helps administrators secure computers whether the computers reside locally, remotely, or in the cloud. It features:

- Baselines
- Security guides
- Support for standalone computers
- Import GPO backups
Lab A: Increasing Security for Server Resources

- Exercise 1: Using Group Policy to Secure Member Servers
- Exercise 2: Auditing File System Access
- Exercise 3: Auditing Domain Logons

Logon Information
Virtual machines 20410C-LON-DC1
          20410C-LON-SVR1
          20410C-LON-SVR2
          20410C-LON-CL1
User name Adatum\Administrator
Password Pa$$w0rd
Estimated Time: 60 minutes
Lab Scenario

Your manager has given you some security-related settings that need to be implemented on all member servers. You also need to implement file system auditing for a file share used by the Marketing department. Finally, you need to implement auditing for domain logons.
Lab Review

• What happens if you configure the Computer Administrators group, but not the Domain Admins group, to be a member of the Local Administrators group on all the computers in a domain?

• Why do you need to not allow local logon on some computers?

• What happens when an unauthorized user tries to access a folder that has auditing enabled for both successful and unsuccessful access attempts?

• What happens when you configure auditing for domain logons for both successful and unsuccessful logon attempts?
Lesson 3: Restricting Software

- What Are Software Restriction Policies?
- What Is AppLocker?
- AppLocker Rules
- Demonstration: Creating AppLocker Rules
What Are Software Restriction Policies?

- Software Restriction Policies (SRPs) allow administrators to identify which apps are allowed to run on client computers.
- SRPs can be based on the following:
  - Hash
  - Certificate
  - Path
  - Zone
- SRPs are applied through Group Policy.
What Is AppLocker?


AppLocker contains capabilities and extensions that:

• Reduce administrative overhead
• Helps administrators control how users can access and use files:
  • .exe files
  • scripts
  • DLLs
  • Windows Installer files (.msi and .msp files)
  • Packaged apps (Windows Store apps)

Benefits of AppLocker:

• Controls how users can access and run all types of apps
• Allows the definition of rules based on a wide variety of variables
• Provides for importing and exporting entire AppLocker policies
AppLocker defines rules based on file attributes such as:

- Publisher name
- Product name
- File name
- File version

**Rule actions**

- Allow or Deny conditions
- Enforce or Audit Only policies
In this demonstration, you will see how to:
- Create a GPO to enforce the default AppLocker Executable rules
- Apply the GPO to the domain
- Test the AppLocker rule
Lesson 4: Configuring Windows Firewall with Advanced Security

• What Is Windows Firewall with Advanced Security?
• Discussion: Why Is a Host-Based Firewall Important?
• Firewall Profiles
• Connection Security Rules
• Deploying Firewall Rules
• Demonstration: Implementing secured network traffic with Windows Firewall
What Is Windows Firewall with Advanced Security?

Windows Firewall is a stateful, host-based firewall that allows or blocks network traffic according to its configuration.
What Is Windows Firewall with Advanced Security?

Windows Firewall is a stateful, host-based firewall that allows or blocks network traffic according to its configuration:

- Supports filtering for both incoming and outgoing traffic
- Integrates firewall filtering and IPsec protection settings
- Enables you to configure rules to control network traffic
- Provides network location-aware profiles
- Enables you to import or export policies

Firewall rules control inbound and outbound traffic.
Discussion: Why Is a Host-Based Firewall Important?

- Why is it important to use a host-based firewall such as Windows Firewall with Advanced Security?
Firewall Profiles

- Firewall profiles are a set of configuration settings that apply to a particular network type.
- The firewall profiles are:
  - Domain
  - Public
  - Private
- Windows Server 2012 includes the ability to have multiple active firewall profiles.
Connection security rules:
• Authenticate two computers before they begin communications
• Secure information being sent between two computers
• Use key exchange, authentication, data integrity, and data encryption (optionally)

How firewall rules and connection rules are related:
• Firewall rules allow traffic through, but do not secure that traffic
• Connection security rules can secure the traffic, but only if a firewall rule was previously configured
Deploying Firewall Rules

You can deploy Windows Firewall rules in the following ways:

• **Manually.** Used during testing, troubleshooting, or for individual computers.

• **Using Group Policy.** The preferred way. Create and test the rules, and then deploy them to a large number of computers.

• **Exporting and importing.** Uses Windows Firewall with Advanced Security. When you import rules, they replace all current rules.

Always test firewall rules in an isolated, non-production environment before you deploy them in production.
In this demonstration, you will see how to:

- Check to see if ICMP v4 is blocked
- Enable ICMP v4 from LON-CL2 to LON-SVR2
- Create a connection security rule so that traffic is authenticated to the destination host
- Validate ICMP v4 after the connection security rule is in place
Lab B: Configuring AppLocker and Windows Firewall

- Exercise 1: Configuring AppLocker Policies
- Exercise 2: Configuring Windows Firewall

Logon Information

Virtual machines
- 20410C-LON-DC1
- 20410C-LON-SVR1
- 20410C-LON-CL1

User name: Adatum\Administrator
Password: Pa$$w0rd

Estimated Time: 60 minutes
Lab Scenario

Your manager has asked you to implement AppLocker to restrict non-standard apps from running. He also has asked you to create new Windows Firewall rules for any member servers running web-based apps.
• You configured an AppLocker rule based on a software path. How can you prevent users from moving the folder containing the software so that they can still run it?

• You would like to introduce a new app that requires the use of specific ports. What information do you need to configure Windows Firewall with Advanced Security, and from what source can you get it?
Module Review and Takeaways

- Review Questions
- Best Practices
- Common Issues and Troubleshooting Tips
- Tools