



Lesson Plans

Administering Security in a Server 2003 Network

(Exam 70-299)

Version 2.0

Table of Contents

Table of Contents.....	1
Course Overview.....	2
Section 1.1: Course Introduction.....	4
Section 1.2: Active Directory.....	5
Section 1.3: Group Policy.....	6
Section 2.1: Roles and Templates.....	7
Section 2.2: Security Settings.....	8
Section 2.3: Account Policies Facts.....	9
Section 3.1: Encryption.....	10
Section 3.2: Certificate Concepts.....	11
Section 3.3: CA Installation.....	12
Section 3.4: Certificate Templates.....	13
Section 3.5: Certificate Autoenrollment.....	14
Section 3.6: Certificate Management.....	15
Section 3.7: CA Management.....	16
Section 4.1: Authentication and Authorization Concepts.....	17
Section 4.2: Authentication.....	18
Section 4.3: Smart Cards.....	19
Section 4.4: Groups.....	20
Section 4.5: Folder and File Access.....	21
Section 4.6: Trusts.....	22
Section 4.7: Digital Signatures.....	23
Section 5.1: IPsec Policies.....	24
Section 5.2: IPsec Troubleshooting.....	25
Section 6.1: Dialup and VPN.....	26
Section 6.2: Remote Access Policies.....	27
Section 6.3: RADIUS.....	28
Section 7.1: IIS Security.....	29
Section 7.2: SSL.....	30
Section 8.1: Software Restrictions.....	31
Section 8.2: Software Update Services.....	32
Section 8.3: Software Deployment.....	33
Section 9.1: Wireless Security.....	34
Section 9.2: Network Zones.....	35
Section 9.3: Server Hardening.....	36
Section 10.1: Auditing.....	37
Section 10.2: Auditing Security Configurations.....	38

Course Overview

This course prepares students for the Implementing and Administering Security in a Microsoft® Windows® Server 2003 Network certification Exam 70-299. It focuses on how to implement and maintain security in the Windows 2003 environment.

Before studying for the Implementing and Administering Security in a Microsoft® Windows® Server 2003 Network exam, you should have extensive working knowledge of the following:

- Active Directory
- Group Policy
- Remote access
- IIS
- NTFS permissions

Module 1 – Security Overview

This module introduces the instructor, prerequisites, and course content. It also provides an overview of Active Directory, group policy, and basic server administration.

Module 2 – Security Templates

Module 2 explains how to enhance security through the use of security templates, security settings, and password and account lockout settings.

Module 3 – Certificates

Module 3 discusses the basics of planning, installing and managing certificates. Topics include, encryption, Certification Authority, Certificate Templates, Certificate Autoenrollment, and CA Management.

Module 4 – Authentication and Authorization

Module 4 covers the concepts of authentication and authorization. Topics also include Kerberos, NTLM, smart cards, group scopes, file system policies, trusts, and digital signatures.

Module 5 – IPSec

In Module 5 students will learn how to configure IPSec to secure data in transmission. Students will learn the tools to analyze and resolve IPSec problems.

Module 6 – Remote Access

Module 6 explains methods to connect to a Remote Access Server (RAS), authentication protocols, authorization through remote access policies, and using a Remote authentication Dial-In User Server (RADIUS) to consolidate remote access policies.

Module 7 – IIS Security

In Module 7 students will learn the five security checks used to provide IIS security to secure transmission of data. Also discussed are Web permissions, SSL, and certificate mapping.

Module 8 – Software Management

Module 8 covers the software management tools used to create software restrictions and deploy service packs. These include Group Policy, path and certificate rules, Software Update Services (SUS), Update.exe, Slipstreaming, WSUS and SMS.

Module 9 – Network Infrastructure Security

Module 9 discusses the basics of wireless security, DMZ, NAT, and server hardening.

Module 10 – Security Auditing

Module 10 explains the tools used to analyze system security. These include MBSA, Security configuration and Analysis, RSoP, and Regedit.

Section 1.1: Course Introduction

Preparation

This section introduces the video instructor, the prerequisites, and the topics that will be covered in this course. Review the prerequisites so that you can make sure the students are prepared to take the course.

Before studying for the Implementing and Administering Security in a Microsoft® Windows® Server 2003 Network exam, students should have extensive working knowledge of the following:

- Active Directory
- Group Policy
- Remote access
- IIS
- NTFS permissions

Time

About 3 minutes

Section 1.2: Active Directory

Preparation

In this section students will review the basics of Active Directory. Students should already have a broad working knowledge of Active Directory before taking this course. They will re-examine the Active Directory components used to organize network resources and simplify management. After finishing this section, students should be able to create an Active Directory structure and change domain and forest functional levels.

Lecture Focus Questions:

- What is the difference between a *tree* and a *forest*?
- When is it appropriate to use multiple forests?
- What are the elements of a *site*?
- What is the difference between the default permissions of the Enterprise Admins group compared to the Domain Admins group?
- Which domain functional level must you use if you want to rename a domain controller?
- What is the difference between domain functional levels and forest functional levels?

Time

About 45 minutes

Lab/Activity

- Structure Active Directory
- Change the Functional Level

Section 1.3: Group Policy

Preparation

This section discusses the basics of Group Policy. Students will review how to apply group policy settings to users or computers. They will implement a Group Policy strategy by creating GPOs and linking them to Active Directory objects.

Lecture Focus Questions:

- When is a computer policy applied?
- Where do you configure *user rights*?
- What happens to a setting that is applied by a GPO at the local level but is not applied by a GPO at the domain level?
- What is the result of GPO settings applied at the site level and separate GPO settings applied at the domain level?
- How is the **Block Inheritance** setting affected by the **No Override** setting?
- How can you create a configuration that creates the same working environment for a user no matter which computer the user logs on to?
- If an OU has four GPOs linked to it, what is the order in which the GPOs are applied?

Time

About 40 minutes

Lab/Activity

- Create and Link a GPO

Section 2.1: Roles and Templates

Preparation

This section covers creating customized security templates based on the role of the computer. Templates can be used to reduce exposure by disabling unnecessary services. After completing this section, students should be able to manage Group Policy by importing security templates, reconfigure security settings through GPOs applied to OUs and apply security templates to meet user requirements.

Windows Server 2003 Objectives

101. Plan security templates based on computer role. Computer roles include SQL Server computer, Microsoft Exchange Server computer, domain controller, Internet Authentication Service (IAS) server, and Internet Information Services (IIS) server.
102. Configure security templates.
103. Deploy security templates.
104. Troubleshoot security template problems.

Lecture Focus Questions:

- If you add an additional security template to a GPO that already contains security settings, what happens to the existing settings?
- If a GPO applied to the local machine requires a user to change passwords every 90 days and a security template applied to the local machine requires the user to change passwords every 45 days, which setting is enforced?
- What may be the effect of applying Setup Security.inf through a GPO?
- What are the differences between *Secure*.inf* and *Hisec*.inf*?
- Which template would you apply in order to allow users to run a legacy application?

Time

About 45 minutes

Lab/Activity

- Import a Template 1
- Import a Template 2

Section 2.2: Security Settings

Preparation

This section overviews the available Security Settings. The Security Setting Categories are presented with a description of each. Students will implement network security standards by configuring user rights assignments and security options.

Windows Server 2003 Objectives

- 102. Configure security templates.
- 403. Plan and configure authorization.

Lecture Focus Questions:

- When do account policies take effect?
- Which security setting allows you to you configure a user's ability to log on to the local machine?
- What is a major difference between user rights and security options?

Time

About 40 minutes

Lab/Activity

- Configure User Rights
- Modify a Security Template
- Configure Security Options

Section 2.3: Account Policies

Preparation

This section discusses how account policies control passwords and login properties. Both password and account lockout settings are explored. Students will learn how to use security templates and GPOs to enforce user account security standards.

Windows Server 2003 Objectives

102. Configure security templates.

Lecture Focus Questions:

- Users in a network have to change their passwords every 30 days, but many users have reported that they simply enter the same password to make the change. Why can they do this?
- What is the effect of setting the minimum password age account policy to 5 days?
- How can you prevent users from creating passwords like desk, mom, chair, or office?
- What is the effect of setting the account lockout policy to 0?
- What type of an account should have the **Password never expires** option set?

Time

About 10 minutes

Lab/Activity

- Configure Account Policies

Section 3.1: Encryption

Preparation

In this section students will learn the basics of encryption. The three typical methods of encryption are described: hashing, symmetric encryption, and asymmetric encryption (PKI). Hashing provides integrity and ensures that data was not modified in transit. Common hashing algorithms are presented.

Lecture Focus Questions:

- What is the difference between symmetric encryption and asymmetric encryption?
- Why does hashing provide data integrity, but not reliable data encryption?
- Why is asymmetric encryption also called PKI?
- What is the relationship between collision vulnerability and a hashing algorithm?

Time

About 25 minutes

Section 3.2: Certificate Concepts

Preparation

This section discusses the concepts of a Certification Authority (CA). A Certification Authority is used to deploy out and issue certificates. Students will learn the factors to consider when planning the certification hierarchy of a certificate authority structure. Also presented are some of the common CA configurations and the conditions for their implementation.

Windows Server 2003 Objectives

404. Install, manage, and configure Certificate Services.

Lecture Focus Questions:

- What advantage does a third-party CA have over an internal CA?
- What does a CA have to possess to issue certificates?
- Why would you choose to take your root CA offline?
- How does a CA verify the validity of the certificates it issues?

Time

About 30 minutes

Section 3.3: CA Installation

Preparation

This section covers how to install a Standalone Root CA and a Subordinate CA. Students will learn the facts to consider when planning a CA installation. One important fact to remind the students is that after installing Certificate Services, you cannot change the computer name or domain membership. Students will have an opportunity to install and configure standalone and subordinate CAs and request, approve, and import a subordinate CA certificate.

Windows Server 2003 Objectives

404. Install, manage, and configure Certificate Services.

Lecture Focus Questions:

- Why must you install a root CA before you install issuing CAs?
- Where does a root CA's certificate come from?
- What type of CA can publish a CRL to Active Directory?
- What must you do to a Windows 2000 forest to implement a Windows 2003 Enterprise CA?

Time

About 40 minutes

Lab/Activity

- Install A Root CA
- Install a Subordinate CA
- Approve a CA Request
- Import a CA Certificate

Section 3.4: Certificate Templates

Preparation

This section discusses how certificate templates can be used to customize and deploy out certificates. Certificate templates are used to reduce the administrative complexity of requesting and issuing certificates. There are two versions for certificate templates. Version 1 templates are fixed templates and version 2 templates can be customized. You can copy a version 1 template to create a version 2 template with similar settings that can be customized. Users and computers must have appropriate permissions to the certificate template in order to request a certificate of that type. Students will learn how to create new certificate templates by duplicating existing templates, modify certificate template permissions, and manage certificate templates deployed on a CA.

Windows Server 2003 Objectives

404. Install, manage, and configure Certificate Services.

Lecture Focus Questions:

- What administrative advantages are provided by certificate templates?
- Which certificate template would you prepare if you wanted to validate a software product from your company?
- What is the difference between version 1 and version 2 templates?
- Why can only Enterprise CAs use certificate templates?
- Which smartcard certificate template should you prepare if users want to encrypt e-mail?

Time

About 30 minutes

Lab/Activity

- Modify Issued Certificate Templates
- Modify a Certificate Template

Section 3.5: Certificate Autoenrollment

Preparation

In this section students will learn how certificates can be managed without user intervention by using autoenrollment. They will learn the minimum requirements to set up autoenrollment and steps to configure it. Students will learn how to modify certificate template permissions and Group Policy settings to enable certificate enrollment

Windows Server 2003 Objectives

404. Install, manage, and configure Certificate Services.

Lecture Focus Questions:

- What permissions must users have for autoenrollment?
- If you want to use autoenrollment, what certificate template version are you required to use? How does this affect your CA requirements?
- You have modified a version 2 certificate template, configured it for autoenrollment, and published it to the CA. Users still cannot autoenroll. Why?
- How does autoenrollment affect certificate renewal?
- When does autoenrollment attempt to renew certificates?
- If you modify a certificate, how can you deploy it to users prior to the renewal period?

Time

About 20 minutes

Lab/Activity

- Enable Autoenrollment

Section 3.6: Certificate Management

Preparation

This section discusses certificate management, which includes approving or denying certificate requests, revoking or unrevoking certificates, and publishing certificate revocation lists (CRLs). Five different methods for requesting certificates are described.

Windows Server 2003 Objectives

404. Install, manage, and configure Certificate Services.

Lecture Focus Questions:

- Which switch must you use to request a certificate using **Certreq**?
- Why is Web-based enrollment easier than using the Certificates snap-in?
- When should you revoke a certificate?
- What is the location from which a CA derives CRL information?
- What is the difference between a delta CRL and a CRL?

Time

About 35 minutes

Lab/Activity

- Manage Certificate Revocation

Section 3.7: CA Management

Preparation

This section covers the tasks to manage CAs. The permissions to manage a CA and its configuration are discussed. Management tasks can be performed through the Certification authority snap-in, or the Certutil.exe command line utility. Students will learn how to modify CA properties and perform a manual backup of a CA.

Windows Server 2003 Objectives

404. Install, manage, and configure Certificate Services.

Lecture Focus Questions:

- To delegate certificate approval to your assistant, what permissions do you need to give her?
- What permissions must your users have to request certificates?
- Why can't you implement key archival in a mixed mode environment?
- What must you restore after your CA server fails in order to get Certificate Services running on a new machine?
- You want to accept all certificates from a CA called CERT1. What kind of constraint can you use?
- What can you do to make sure two separate root CAs that need to trust each other's certificates achieve that trust?

Time

About 30 minutes

Lab/Activity

- Back Up a CA

Section 4.1: Authentication and Authorization Concepts

Preparation

Familiarize yourself with the concepts of authorization and authentication. Authentication determines that you are who you say you are and not a malicious user. Three authentication methods are discussed: what you know, what you have, and who you are. After authentication is determined authorization determines what you will be able to access and the level of access. Students will learn how to view access token information.

Lecture Focus Questions:

- What is the relationship between authorization and authentication?
- How can you secure your network against malicious impersonation?
- What does a number that begins with S-1-5-21 identify?
- What does an access token contain?
- If you allow users to access only the applications they need to do their jobs, what kind of access are you allowing?

Time

About 15 minutes

Section 4.2: Authentication

Preparation

This section discusses the two authentication mechanisms (Kerberos and NTLM) for logging on to the server or domain and when to use them. Delegated authentication allows a network service to assume the identity of a user and initiate requests to other services on behalf of the user. Students will learn how to configure NTLM authentication using Group Policy and manage delegated authentication for users and computers.

Windows Server 2003 Objectives

401. Plan and configure authentication.

Lecture Focus Questions:

- What advantages does Kerberos have over NTLM?
- With Kerberos, what is the function of a ticket?
- When is it appropriate to use NTLM v2 rather than Kerberos?
- Which policy setting would you use to disable ticket expiration?
- What is the best method for enforcing Kerberos policy settings?
- When would you use certificates rather than Kerberos?
- Which policy should you configure to prevent a user from using delegated authentication?
- What types of computers should not be trusted for delegated authentication?

Time

About 35 minutes

Lab/Activity

- Enforce NTLM v2
- Enable Delegated Authentication

Section 4.3: Smart Cards

Preparation

In this section students will learn how smart cards are used to provide secure, multi-factor authentication. Also discussed are certificate template types used for smart card administration. Students will learn how to configure certificate templates for smart card authentication and autoenrollment, and how to use Group Policy to enforce smart card authentication policies.

Windows Server 2003 Objectives

401. Plan and configure authentication.

Lecture Focus Questions:

- Why is an enrollment agent important for smart card use?
- What setting can you configure to prevent users from leaving machines running after they log on with their smart cards?
- What hardware requirements do smart cards have?
- Which certificate templates should you modify to implement smart card authentication?

Time

About 20 minutes

Lab/Activity

- Create a Certificate for Smart Cards
- Require Smart Cards for Logon

Section 4.4: Groups

Preparation

This section reviews implementing groups to reduce administrative overhead and to increase security by controlling access to resources. Three types of group scopes are discussed with their membership and use. Recommended strategies for managing users, groups, and permissions is also included. Students will learn how to manage group strategy by organizing groups according to user roles and how to control local group membership using restricted groups in Group Policy.

Windows Server 2003 Objectives

- 102. Configure security templates.
- 402. Plan group structure.

Lecture Focus Questions:

- What is the difference between a global group and a universal group?
- When is it appropriate to use universal groups?
- Where should you assign permissions to access resources when using UGLR or (J)UGULR?
- What is the difference between security and distribution groups?

Time

About 70 minutes

Lab/Activity

- Implement a Group Strategy 1
- Implement a Group Strategy 1
- Configure Restricted Groups

Section 4.5: Folder and File Access

Preparation

This section discusses using File System policies in Group Policy to control NTFS permissions on folders or files that exist on multiple computers using File System policies in Group Policy. Also discussed is how the Encrypting File System (EFS) is used to protect data on files and folders stored on NTFS partitions. In this section students will learn how to manage file system access using file restriction in Group Policy and how to implement DRAs for EFS.

Windows Server 2003 Objectives

102. Configure security templates.
403. Plan and configure authorization.

Lecture Focus Questions:

- How does inheritance affect permission assignments?
- Which account is the default EFS recovery agent?
- What is the biggest difference between EFS in Windows 2000 and Windows 2003?
- What can you do to open an EFS encrypted file if the owner is not available?

Time

About 70 minutes

Lab/Activity

- Restrict a Folder
- Modify the DRA Certificate Template
- Add OU DRAs

Section 4.6: Trusts

Preparation

In this section students will learn about using a trust relationship to enable members in one domain to access resources in another domain. Students will learn how to create trust relationships between domains and between forests.

Windows Server 2003 Objectives

401. Plan and configure authentication.

Lecture Focus Questions:

- What is the relationship between the direction of trust and the direction of access?
- If you have users in three domains that need access to resources in each domain, which kind of a trust do you need to establish?
- When should you use a shortcut trust?
- What is the difference between the creation of tree root trusts and forest root trusts?
- Which authentication method allows you to secure resources in a forest trust?

Time

About 60 minutes

Lab/Activity

- Create an External Trust
- Create a Forest Root Trust
- Create a Shortcut Trust

Section 4.7: Digital Signatures

Preparation

This section presents how digital signatures are used to provide integrity and nonrepudiation of data

Windows Server 2003 Objectives

403. Plan and configure authorization.

Lecture Focus Questions:

- How can a digital signature confirm the origin of a message?
- How can a digital signature help you feel confident that the message wasn't altered?

Time

About 15 minutes

Section 5.1: IPSec Policies

Preparation

This section discusses using Internet Protocol Security (IPSec) policies to control IPSec. The characteristics of Windows default IPSec policies are described. IPSec policies use rules to define the type of traffic secured with IPSec. Settings that can be configured for a rule are presented. Students will learn how to analyze IPSec traffic using IPSec Monitor and resolve IPSec problems using troubleshooting tools.

Windows Server 2003 Objectives

301. Plan IPSec deployment.
302. Configure IPSec policies to secure communication between networks and hosts. Hosts include domain controllers, Internet Web servers, databases, e-mail servers, and client computers.
303. Deploy and manage IPSec policies.

Lecture Focus Questions:

- What happens if a client configured to use IPSec contacts a server that is not configured to use IPSec?
- What happens if a server configured to request IPSec is contacted by a client that does not use IPSec?
- Where do you configure IPSec to apply only to remote access connections?
- How does tunnel mode affect the need for a client to be able to use IPSec?

Time

About 70 minutes

Lab/Activity

- Enforce IPSec
- Create an IPSec Certificate Template

Section 5.2: IPSec Troubleshooting

Preparation

In this section students learn how to resolve IPSec problems using troubleshooting tools. Students will need to understand how the three modes of the IPSec driver affects the way IPSec policies are applied. Students will learn how to analyze IPSec traffic using IPSec Monitor.

Windows Server 2003 Objectives

- 301. Plan IPSec deployment.
- 304. Troubleshoot IPSec.

Lecture Focus Questions:

- Which IPSec logging level records outbound per-packet drop events?
- Where do you go to view IPSec logging events?
- Where do you enable Oakley logging?
- What is the difference between Main Mode and Quick Mode?

Time

About 35 minutes

Section 6.1: Dialup and VPN

Preparation

This section discusses two ways to connect to a Remote Access Server (RAS): Dialup and VPN. Dialup uses SLIP and PPP connection protocols. VPN uses a VPN tunneling protocol to protect data as it travels through an unprotected network. Also discussed, are authentication protocols used to ensure that remote users have the necessary credentials for remote access. Students will learn how to configure remote access and VPN connections.

Windows Server 2003 Objectives

307. Configure security for remote access users.

Lecture Focus Questions:

- Which protocol should you choose to authenticate Windows XP machines to your new wireless network?
- If you have a system that includes non-Microsoft machines along with Windows 9x and Windows 2000 machines, which authentication protocol should you use?
- How does a *service profile* facilitate network connections?
- What does a *service profile* contain?

Time

About 45 minutes

Lab/Activity

- Configure VPN Ports

Section 6.2: Remote Access Policies

Preparation

In this section students will learn how authorization is handled through remote access policies. Students will learn how to apply the principles of RAPCAP to create remote access connections for specific users with specific needs. They will also learn how to analyze remote access connection policies to isolate and fix connection problems or irregularities.

Windows Server 2003 Objectives

307. Configure security for remote access users.

Lecture Focus Questions:

- Where are Remote Access Policies stored?
- What is the difference between conditions and profile settings in a remote access policy?
- If you have conditions that allow all users access during business hours and conditions that all sales users access any time, why should you put the sales conditions first?

Time

About 45 minutes

Lab/Activity

- Create a Remote Access Policy 1
- Create a Remote Access Policy 2
- Troubleshoot Remote Access Policies 1
- Troubleshoot Remote Access Policies 2
- Troubleshoot Remote Access Policies 3

Section 6.3: RADIUS

Preparation

This section covers using a Remote Authentication Dial-In User Service (RADIUS) server to consolidate remote access policies. Policies stored on the RADIUS server can then be applied to multiple remote access servers. Students will learn how to configure RADIUS clients in IAS and how to configure remote access policies on an IAS server.

Windows Server 2003 Objectives

307. Configure security for remote access users.

Lecture Focus Questions:

- How can you centralize remote access policies?
- What is the relationship between the remote access server and the RADIUS server?
- What is the relationship between RADIUS and IAS?
- How does a RADIUS client authenticate to a RADIUS server?
- What is the difference between a remote access client and a RADIUS client?

Time

About 30 minutes

Lab/Activity

- Configure a RADIUS Server
- Configure a RADIUS Client

Section 7.1: IIS Security

Preparation

This section discusses the five security checks that attempts to get to a Web page must go through. Also discussed are authentication methods available with IIS and IIS permissions you can set for Web sites or Web folders. Students will learn how to configure Web site, virtual directory, or file authentication. They will also learn how to secure Web resources using Web and NTFS Permissions.

Windows Server 2003 Objectives

401. Plan and configure authentication.

Lecture Focus Questions:

- What are the features of the Basic Authentication?
- What is the disadvantage of Integrated Windows Authentication?
- If you grant the NTFS Full Control permission to a folder and the IIS Read and Write permissions to the same folder for the same group, what is the group's effective set of permissions?

Time

About 40 minutes

Lab/Activity

- Configure Web Site Authentication
- Configure Virtual Directory Permissions

Section 7.2: SSL

Preparation

In this section students will learn how to use SSL to provide secure transmissions of data. Three different methods of certificate mapping are presented; One-to-one, Many-to-one, and Directory Service. Students will learn how to request a Web server certificate, require SSL for a Web site and configure certificate mapping.

Windows Server 2003 Objectives

- 306. Deploy, manage, and configure SSL certificates, including uses for HTTPS, LDAPS, and wireless networks. Considerations include renewing certificates and obtaining self-issued certificates instead of publicly issued certificates.
- 401. Plan and configure authentication.

Lecture Focus Questions:

- What is the difference between 1-to-1 mapping and many-to-1 mapping?
- You configured the server to accept client certificates. Your clients still cannot authenticate. What can you do to fix the problem?
- What type of mapping can you use to allow Active Directory to store the certificates?
- You've been told to allow clients who have certificates from three trusted CAs to authenticate to the system. What can you do to ease your administrative burden?
- How can you add security to basic authentication?

Time

About 30 minutes

Lab/Activity

- Enable SSL
- Configure Client Mapping

Section 8.1: Software Restrictions

Preparation

This section discusses how software restrictions are used to control which software is allowed for computers and users. Students will learn how to create and configure software restrictions in Group Policy and configure software restrictions using path and certificate rules.

Windows Server 2003 Objectives

105. Configure additional security based on computer roles. Server computer roles include SQL Server computer, Exchange Server computer, domain controller, Internet Authentication Service (IAS) server, and Internet Information Services (IIS) server. Client computer roles include desktop, portable, and kiosk.

Lecture Focus Questions:

- Several users on your network downloaded a music sharing application to their local machines. You want to restrict the software. Which rule type should you use if users store the application in different locations?
- After you configure a certificate rule, what else must you do to make the rule take effect?
- What is the advantage to applying software restrictions through their own GPOs?
- Which option do you use to verify that a publisher's certificate has not expired?
- What type of software is controlled through Internet zone rule restrictions?

Time

About 60 minutes

Lab/Activity

- Restrict Running Scripts
- Control User Applications
- Allow Signed Software

Section 8.2: Software Update Services

Preparation

This section discusses using Software Update Services (SUS) to configure where updates are stored, who approves updates, and how to distribute load. Students will learn how to use Group Policy to manage SUS settings.

Windows Server 2003 Objectives

201. Plan the deployment of service packs and hotfixes.
203. Deploy service packs and hotfixes.

Lecture Focus Questions:

- Why would you choose to have clients download updates locally rather than from Microsoft?
- If your large organization's security policy requires client computers to have the same configuration, which SUS configuration should you deploy?
- If your users continually ignore your directive to leave their machines on at night when updates download and install, what can you do to make sure their machines still receive updates?
- Which policy allows you to send different sets of updates to different sets of users?

Time

About 45 minutes

Lab/Activity

- Enforce SUS

Section 8.3: Software Deployment

Preparation

This section presents several different methods to deploy service packs. They include; Update.exe, Slipstreaming, Group Policy, SUS, WSUS, and SMS. Four types of file extensions used with installer packages are discussed so the student will understand the purpose of each type. Also discussed, is how Group Policy can be used to either assign or publish software. Assigning software installs it automatically. Publishing software makes it available for installation by adding it to Add/Remove Programs. In this section students will also learn how to use Group Policy to distribute software.

Windows Server 2003 Objectives

201. Plan the deployment of service packs and hotfixes.
203. Deploy service packs and hotfixes.

Lecture Focus Questions:

- Why would you install a non-critical, recommended update?
- What's the difference between a *service pack* and a *security rollup package*?
- Why might you decide *not* to install a critical update?
- What's the difference between a recommended update and a feature pack?
- Where would you find the Knowledge Base article number for an update you recently installed?
- What is the difference between assigning and publishing software?

Time

About 40 minutes

Lab/Activity

- Distribute a Patch
- Distribute Antivirus Software

Section 9.1: Wireless Security

Preparation

This section introduces the basics of wireless security including; network types, methods of authentication, and methods of encryptions. Students will learn how to configure wireless access using 802.1x Authentication.

Windows Server 2003 Objectives

305. Plan and implement security for wireless networks.

Lecture Focus Questions:

- How do WEP and WPA differ?
- If you have 5 clients (4 Windows XP, 1 Windows Me), which encryption solution should you choose?
- In 802.1x authentication, what is the RADIUS client?
- Why would you choose PEAP-EAP-TLS over EAP-TLS?

Time

About 70 minutes

Lab/Activity

- Create a Wireless Certificate Template
- Configure Wireless Access on the IAS Server
- Create a Wireless Network Policy

Section 9.2: Network Zones

Preparation

This section discusses a demilitarized zone (DMZ) and Network Translation (NAT). DMZ is used to protect publicly accessible resources and help isolate resources from the internal network. NAT is used to connect a private network to the Internet without obtaining registered address for every host.

Windows Server 2003 Objectives

105. Configure additional security based on computer roles. Server computer roles include SQL Server computer, Exchange Server computer, domain controller, Internet Authentication Service (IAS) server, and Internet Information Services (IIS) server. Client computer roles include desktop, portable, and kiosk.

Lecture Focus Questions:

- Where should a Web server be placed when using a DMZ? Where would you place a database server to allow customers to look up product information?
- How does NAT provide security for networks?
- Why are VPNs sometimes incompatible with NAT?

Time

About 25 minutes

Section 9.3: Server Hardening

Preparation

This section covers the general rules to use to secure devices and software by reducing the security exposure and tightening security controls. Students will learn how to use System Services in Group Policy to prevent unnecessary services from running.

Windows Server 2003 Objectives

105. Configure additional security based on computer roles. Server computer roles include SQL Server computer, Exchange Server computer, domain controller, Internet Authentication Service (IAS) server, and Internet Information Services (IIS) server. Client computer roles include desktop, portable, and kiosk.

Lecture Focus Questions:

- What can you do to secure the FTP service?
- What can you use to track DHCP traffic?
- How are security considerations different for DHCP and DNS servers?
- What security advantage does network access quarantine provide?
- What security vulnerability does the SA account pose?
- Which service permission would you grant to allow a user to modify the startup behavior of a service?

Time

About 25 minutes

Lab/Activity

- Restrict Services

Section 10.1: Auditing

Preparation

This section discusses the concept of auditing as an element of administration. Auditing allows the administrator to monitor access or attempted access of resources. Students will learn how to configure auditing using Group Policy.

Windows Server 2003 Objectives

102. Configure security templates.
105. Configure additional security based on computer roles. Server computer roles include SQL Server computer, Exchange Server computer, domain controller, Internet Authentication Service (IAS) server, and Internet Information Services (IIS) server. Client computer roles include desktop, portable, and kiosk.

Lecture Focus Questions:

- What is the difference between auditing for success and auditing for failure?
- What is the difference between Account Logon and Logon auditing?
- What additional step must you complete in order to audit NTFS file access?
- Which IIS log file type allows you to customize the log file contents?
- What are the advantages for using an ODBC format for IIS logging?

Time

About 50 minutes

Lab/Activity

- Configure Auditing
- Audit the Certificate Authority

Section 10.2: Auditing Security Configurations

Preparation

This section discusses several of the tools available to analyze security vulnerabilities on the network. Tools include patch level assessment tools and security auditing tools.

Windows Server 2003 Objectives

104. Troubleshoot security template problems.
105. Configure additional security based on computer roles. Server computer roles include SQL Server computer, Exchange Server computer, domain controller, Internet Authentication Service (IAS) server, and Internet Information Services (IIS) server. Client computer roles include desktop, portable, and kiosk.
202. Assess the current status of service packs and hotfixes. Tools include MBSA and the MBSA command-line tool.

Lecture Focus Questions:

- What is the difference between MBSA 1.2.1 and MBSA 2.0?
- When using MBSA, where can you find the results of a scan you do locally?
- How can you find out if your users are creating strong passwords?
- What can **Regedit** tell you about Group Policy?
- What does RSoP tell you that you can't otherwise learn by using Security Configuration and Analysis to compare a computer to a template?

Time

About 65 minutes