



Lesson Plans

Designing Security for a Server 2003 Network

(Exam 70-298)

Version 2.0

Table of Contents

Table of Contents	1
Course Overview	2
Course Introduction.....	3
Section 1.1: Identifying Security Requirements	4
Section 1.2: Design and Implementation.....	5
Section 2.1: Active Directory.....	6
Section 2.2: Trusts.....	7
Section 2.3: Public Key Infrastructure (PKI).....	8
Section 2.4: Administration	9
Section 2.5: Update Infrastructure	10
Section 3.1: Firewalls.....	11
Section 3.2: Data Transmission	12
Section 3.3: Wireless Security	13
Section 3.4: IIS Security	14
Section 3.5: Server Roles.....	15
Section 3.6: External Access.....	16
Section 4.1: Group Strategy	17
Section 4.2: Access Control.....	18
Section 4.3: Auditing	19
Section 5.1: Client Authentication.....	20
Section 5.2: Remote Access.....	21
Section 5.3: Securing Clients	22

Course Overview

This course prepares students for the Designing Security for the Microsoft® Windows® Server 2003 Environment certification Exam 70-298. It focuses on how to design security in the Windows 2003 environment.

Course Overview

This introduces the instructor and prerequisites for the course.

Module 1 – Conceptual Design

This module introduces the basics of analyzing, designing and implementing security for a business.

Module 2 – Logical Design

Module 2 explains how to logically design security using Active Directory, trusts, Public Key Infrastructure, remote administration and automatic updates.

Module 3 – Physical Design

Module 3 discusses the physical strategies used in designing security. Topics include; firewalls, securing data transmission, wireless security, IIS security, server roles, server templates, and Extranets.

Module 4 – Access Control Strategy

Module 4 covers group strategy, access control strategy, and auditing strategy.

Module 5 – Client Infrastructure Design

In Module 5 students will learn about design issues for client authentication, remote access, and securing client workstations.

Course Introduction

Preparation

The video introduces the video instructor and the prerequisites for this course. Review the prerequisites with the students to ensure the students are prepared to take the course.

Before studying for the Exam 70-298: Designing Security for a Microsoft® Windows® Server 2003 Environment exam, students should have extensive working knowledge of and pass the following exams:

- MCSE core courses exams
 - Exam 70-290: Managing and Maintaining a Microsoft® Windows® Server 2003 Environment
 - Exam 70-291: Implementing, Managing, and Maintaining a Microsoft® Windows® Server 2003 Network Infrastructure
 - Exam 70-293: Planning and Maintaining a Microsoft® Windows® Server 2003 Network Infrastructure
 - Exam 70-294: Planning, Implementing, and Maintaining a Microsoft® Windows® Server 2003 Active Directory Infrastructure
- 70-299 Implementing Microsoft® Windows® Server 2003 Network

Time

About 3 minutes

Section 1.1: Identifying Security Requirements

Preparation

In this section students will learn the basics of analyzing existing security, environment and technical requirements of a business. Students are directed to which elements they should consider when doing the business and technical analysis.

Designing Security Objectives

101. Analyze business requirements for designing security. Considerations include existing policies and procedures, sensitivity of data, cost, legal requirements, end-user impact, interoperability, maintainability, scalability, and risk.
 - Analyze existing security policies and procedures.
 - Analyze the organizational requirements for securing data.
 - Analyze the security requirements of different types of data.

Lecture Focus Questions:

- How might legal requirements applicable to the company or the location affect your security design?
- How does understanding the workflow help you to identify groups and access needs?
- What are some of the technical issues that might mean that you would have to modify the security design?
- How does the administrative approach affect the security design?

Time

About 15 minutes

Section 1.2: Design and Implementation

Preparation

In this section students will discover how to create a security design and implement the plan. Students will learn the security principals to consider when designing security and the basic phases of the design framework. They will also learn how to test and maintain the security plan.

Designing Security Objectives

101. Analyze business requirements for designing security. Considerations include existing policies and procedures, sensitivity of data, cost, legal requirements, end-user impact, interoperability, maintainability, scalability, and risk.
 - Analyze risks to security within the current IT administration structure and security practices.
102. Design a framework for designing and implementing security. The framework should include prevention, detection, isolation, and recovery.
 - Predict threats to your network from internal and external sources.
 - Design a process for responding to incidents.
 - Design segmented networks.
 - Design a process for recovering services.
103. Analyze technical constraints when designing security.
 - Identify capabilities of the existing infrastructure.
 - Identify technology limitations.
 - Analyze interoperability constraints.

Lecture Focus Questions:

- What is the difference between a *threat* and a *risk*?
- Why is it impossible to eliminate all risk?
- When might accepting risk be a better choice than deploying a countermeasure to reduce the risk?
- Why is *availability* a security concern, even if data has not been lost or compromised?
- How does the *principle of least privilege* differ from *separation of duties*?
- What are some key components of a security policy?

Time

About 20 minutes

Section 2.1: Active Directory

Preparation

This section is an overview of Active Directory, group policy and the design concepts to consider. Students should already have a thorough knowledge of Active Directory before taking this course.

Designing Security Objectives

- 202. Design a logical authentication strategy.
 - Design forest and domain trust models.
- 401. Design an access control strategy for directory services.
 - Create a delegation strategy.

Lecture Focus Questions:

- Which conditions require you to create separate domains?
- When must you create separate forests?
- Why is tree design typically *not* a concern when finalizing the Active Directory structure?
- Why would you typically move computer accounts out of the Computers container?
- What type of trust exists between domains in the same forest?
- How can you enforce desktop settings on Windows 98 and NT systems?

Time

About 25 minutes

Section 2.2: Trusts

Preparation

This section covers the basics of trusts. Trusts enable members of one domain to access resources in another domain. The different types of trust and their characteristics are presented along with the two different types of trust authentication.

Designing Security Objectives

202. Design a logical authentication strategy.
 - Design certificate distribution.
 - Design forest and domain trust models.

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 30 minutes

Section 2.3: Public Key Infrastructure (PKI)

Preparation

This section discusses PKI designs. It covers the elements such as the CA hierarchy role, CA type, and the CA access that must be considered when planning a certificate authority structure. Also discussed are the methods for distributing certificates and the requirements to setup certificate autoenrollment.

Designing Security Objectives

201. Design a public key infrastructure (PKI) that uses Certificate Services.
 - Design a certification authority (CA) hierarchy implementation. Types include geographical, organizational, and trusted.
 - Design enrollment and distribution processes.
 - Establish renewal, revocation and auditing processes.
 - Design security for CA servers.

102. Configure security templates.

Lecture Focus Questions:

- Why should you typically take the root CA offline?
- In a typical CA hierarchy, why isn't the root CA usually an Enterprise CA?
- What are the prerequisites for using certificate autoenrollment?
- In addition to defining a certificate template and modifying the permissions, what else must you do before the certificate can be issued?
- When would you typically get a certificate from a third-party CA, even if you have an internal CA hierarchy established?
- Which type of CA is normally configured to issue user and computer certificates?

Time

About 30 minutes

Section 2.4: Administration

Preparation

This section discusses the elements to consider when designing a remote administration strategy. Also discussed, are security issues that are related to remote administrative tools and guidelines for designing an administrative strategy.

Designing Security Objectives

- 203. Design security for network management.
 - Manage the risk of managing networks.
 - Design the administration of servers by using common administration tools. Tools include Microsoft Management Console (MMC), Terminal Server, Remote Desktop for Administration, Remote Assistance, and Telnet.
 - Design security for Emergency Management Services.
- 401. Design an access control strategy for directory services.
 - Create a delegation strategy.
 - Design a permission structure for directory service objects.

Lecture Focus Questions:

- How does granting a user Full Control over an OU violate the principle of least privilege?
- What tool can you use to simplify Active Directory permission assignments?
- What are the limitations of using the Remote Administration Website?
- How is the communication channel secured when using Remote Desktop? MMC consoles?
- Why do many organizations give administrators two user accounts?
- How can you perform administrative tasks when you are logged in as a different user without logging out first?

Time

About 25 minutes

Section 2.5: Update Infrastructure

Preparation

This section discusses the different methods used to automate updates for operating system and software. Also discussed, are Software Update Services (SUS) concepts, benefits, and uses the students should consider when designing an SUS infrastructure. Students will also learn about the tools to use to check software patch levels.

Designing Security Objectives

205. Design a security update infrastructure.
 - Design a Software Update Services (SUS) infrastructure.
 - Design Group Policy to deploy software updates.
 - Design a strategy for identifying computers that are not at the current patch level.

Lecture Focus Questions:

- What are two main advantages to using Software Update Services (SUS) over the Windows Update Website?
- Which tools can you use to distribute updates to custom software that you have developed yourself?
- How can you use a single SUS server to approve updates for different groups of computers?
- What is the difference between **Mbsacli** and **Secedit**? Which tool scans for missing operating system patches?

Time

About 30 minutes

Section 3.1: Firewalls

Preparation

In this section students will learn the basics of designing a firewall solution. Any network attached to the Internet should implement a firewall to control external traffic by blocking or allowing it as configured by the packet filters. Also discussed, is how a Demilitarized Zone (DMZ) is used to protect publicly accessed resources and help isolate those resources from your internal network.

Designing Security Objectives

301. Design network infrastructure security.
- Specify the required protocols for a firewall configuration.
 - Design IP filtering.

Lecture Focus Questions:

- How can NAT provide limited firewall functionality?
- Why might you implement IPSec filters even when you do not want to allow or enforce IPSec?
- What is an advantage of using IPSec filters over defining packet filters?
- What type of servers should be placed inside the demilitarized zone?
- Where should servers such as SQL and Exchange servers be placed in a firewall design?

Time

About 15 minutes

Section 3.2: Data Transmission

Preparation

This section discusses the concepts of securing data during transmission. A brief overview is given of several methods that can be used and then it focuses in on IPSec, VPN and Demand-dial strategies.

Designing Security Objectives

301. Design network infrastructure security.
 - Design an IPSec policy.
 - Design security for data transmission.
305. Design security for communication between networks.
 - Select protocols for VPN access.
 - Design VPN connectivity.
 - Design demand-dial routing between internal networks.

Lecture Focus Questions:

- How can you force an IIS server to use TLS instead of SSL?
- Which protocol is used with L2TP to provide data encryption?
- Which method is typically used on a Web server to protect data transmissions?
- Which method is typically used between two computers on a LAN to protect data transmissions?
- Which method is typically used between devices communicating through the Internet to protect data transmissions?
- What are the conditions for using Kerberos for authentication with IPSec?
- Which protocol used with IPSec would you choose to provide both data encryption and authentication, AH or ESP?
- What type of authentication methods are supported when using IPSec with L2TP?
- What are the configuration tasks required to establish a demand dial connection?

Time

About 20 minutes

Section 3.3: Wireless Security

Preparation

This section covers elements of designing a wireless network. Discussed are wireless types, authentication mechanisms and encryption methods. 802.1x Authentication is discussed in greater detail than other authentication methods.

Designing Security Objectives

- 302. Design security for wireless networks.
 - Design public and private wireless LANs.
 - Design 802.1x authentication for wireless networks.

Lecture Focus Questions:

- Why is dynamic WEP more secure than static WEP?
- How can you protect wireless communications when connecting to a public wireless network such as at an airport or a hotel lobby?
- What type of servers must you have on your network in order to implement 802.1x authentication?
- Why would you choose PEAP-EAP-TLS over EAP-TLS?
- When might you use PEAP-EAP-MSCHAPv2 over PEAP-EAP-TLS when configuring 802.1x authentication?
- What are two methods you can use to automate configuring client wireless connections?

Time

About 30 minutes

Section 3.4: IIS Security

Preparation

This section discusses the considerations for locking down an IIS Server. The five security checks a client must go through before they can access an IIS server and a Web page is discussed. Also discussed are the three basic categories of authentication. SSL, a method to provide a secure transmission of data, and certificate mapping, is also covered.

Designing Security Objectives

- 303. Design user authentication for Internet Information Services (IIS).
 - Design user authentication for a Web site by using certificates.
 - Design user authentication for a Web site by using IIS authentication.
 - Design user authentication for a Web site by using RADIUS for IIS authentication.
- 304. Design security for Internet Information Services (IIS).
 - Design security for Web sites that have different technical requirements by enabling only the minimum required services.
 - Design a monitoring strategy for IIS.
 - Design an IIS baseline that is based on business requirements.
 - Design a content management strategy for updating an IIS server.

Lecture Focus Questions:

- What limitation of using Windows Integrated authentication is overcome by using Digest authentication?
- How must user passwords be stored in Active Directory when using Digest authentication? How does Advanced Digest overcome this requirement?
- What should you do to protect user logon credentials if you must support Basic authentication?
- What type of certificates are required to enable SSL on a Web server?
- How can you secure FTP traffic with IIS 6.0?
- How are encrypted files sent when copied to a WebDAV folder? How does this make using SSL unnecessary?
- What type of IIS server logging sends data to a SQL database?

Time

About 35 minutes

Section 3.5: Server Roles

Preparation

In this section students will learn how to design security to lock down security on server roles. Also discussed are the purposes, types and methods of implementing security templates.

Designing Security Objectives

307. Design security for servers that have specific roles. Roles include domain controller, network infrastructure server, file server, IIS server, terminal server, and POP3 mail server.
 - Define a baseline security template for all systems.
 - Create a plan to modify baseline security templates according to role.

Lecture Focus Questions:

- What is the most efficient way to apply security settings to multiple computers?
- How can you apply security settings to a single computer?
- How can you make sure that current security settings on a computer match the settings in a security template?
- What feature should be disabled on e-mail servers to prevent forwarding spam?

Time

About 35 minutes

Section 3.6: External Access

Preparation

This section discusses using an Extranet to allow specified users who are not within your network to access your resources. Access to the Extranet is controlled through firewalls and appropriate authentication. Also discussed is using qualified subordination to control which certificates are issued and the clients to which certificates are issued.

Designing Security Objectives

306. Design security for communication with external organizations.
 - o Design an extranet infrastructure.
 - o Design a strategy for cross-certification of Certificate Services.

Lecture Focus Questions:

- Why are forest root trusts typically not used for extranet access?
- If users in domain A need to access resources in domain B, what is the direction of trust required?
- How do you establish trust between certification hierarchies in Windows 2003? How does this differ from the process you would use with Windows 2000?

Time

About 20 minutes

Section 4.1: Group Strategy

Preparation

In this section the students will learn the concept of using groups to create a more secure access of resources. Types of groups, group scopes and strategies to use groups are all discussed.

Designing Security Objectives

401. Design an access control strategy for directory services.
 - Design the appropriate group strategy for accessing resources.

Lecture Focus Questions:

- When assigning permissions to a resource, which group type will typically be placed on the access control list (ACL) for the object?
- How does the domain mode affect the availability of group scopes?
- When is it appropriate to use universal groups? Why don't you automatically use universal groups when multiple domains are involved?
- How can you prevent any user from being added to a local group?
- Why doesn't the Member of setting in a restricted group restrict group membership to only the listed groups?

Time

About 15 minutes

Section 4.2: Access Control

Preparation

This section discusses designing an access control strategy. Windows uses Access Control Lists (ACLs) to control access to resources such as files, printer, and Active Directory objects. It also discusses concerns when locking down the registry. Students will learn factors to consider when deciding whether to enable or disable the use of an Encrypting File System (EFS).

Designing Security Objectives

402. Design an access control strategy for files and folders.
 - Design a strategy for the encryption and decryption of files and folders.
 - Design a permission structure for files and folders.
 - Design security for a backup and recovery strategy.
403. Design an access control strategy for the registry.
 - Design a permission structure for registry objects.

Lecture Focus Questions:

- What is the recommended method for assigning permissions to everyone on a network?
- What is the easiest way to manage Active Directory object permissions for delegated administrative permissions?
- How are registry permissions similar to NTFS permissions?
- What type of auditing would you use to audit registry access?
- How do you enforce 3DES encryption with EFS?
- What are the advantages of using a PKI with EFS?
- How can you recover (unencrypt) encrypted files without a data recovery agent (DRA)?
- What actions must you take on a server to enable users to save encrypted files on the server?
- How can you protect encrypted files while they are being copied to a network share?

Time

About 20 minutes

Section 4.3: Auditing

Preparation

In this section students will learn the basics of designing an auditing strategy. Students will learn the main points that should be considered; deployment, minimizing auditing, and tracking exactly what is audited.

Designing Security Objectives

401. Design an access control strategy for directory services.
 - Analyze auditing requirements.
402. Design an access control strategy for files and folders.
 - Analyze auditing requirements.
403. Design an access control strategy for the registry.
 - Analyze auditing requirements.

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?
- How does Security log file management affect the usefulness of configuring auditing?
- When would you not enable auditing in a GPO applied to the domain or a specific OU?

Time

About 15 minutes

Section 5.1: Client Authentication

Preparation

This section discusses design issues of client authentication such as; implementing single sign-on, deploying Active Directory clients for pre-2000 machines, implementing a secure LAN Manager authentication, and implementing multi-factor authentication. Students will also learn about authentication protocols that are used to securely transmit passwords from client to server. Also discussed is how account policies can be used to improve security by enforcing password and account lockout settings.

Designing Security Objectives

501. Design a client authentication strategy.
 - Analyze authentication requirements.
 - Establish account and password security requirements.

Lecture Focus Questions:

- How can you enable the use of NTLM v2 on Windows 9x clients?
- What are the requirements for implementing smart cards on a Windows network?
- What type of certificates are required by a smart card enrollment agent?
- How do you require smart cards for specific users or computers?
- Where are Account Policies configured?
- What must you do if you have two divisions with different Account Policies requirements?
- When would you need to enable reversible encryption for passwords?

Time

About 20 minutes

Section 5.2: Remote Access

Preparation

In this section students learn the authentication methods and authorization processes for remote access. Remote access policies allow or deny remote access connection requests based upon connection specific elements such as group membership, time of day, or the type of connection. Students will learn how the acronym RADIUS will help them to remember the three steps to authorization for access to resources.

Designing Security Objectives

502. Design a security strategy for client remote access.
 - o Design remote access policies.
 - o Design access to internal resources.
 - o Design an authentication provider and accounting strategy for remote network access by using Internet Authentication Service (IAS).

Lecture Focus Questions:

- Why is the remote access policy order important when designing remote access policies? What is the general rule to follow when determining which policies should be at the top of the list?
- How can you centralize remote access policies on a single server when multiple remote access servers are being deployed?
- When using a RADIUS solution, what type of device is identified as a RADIUS *client*?

Time

About 20 minutes

Section 5.3: Securing Clients

Preparation

This section summarizes the considerations you should be aware of while planning client workstation security. These include: computer roles, Active Directory and group policy, security templates, administrative templates, software restrictions, and physical security.

Designing Security Objectives

503. Design a strategy for securing client computers. Considerations include desktop and portable computers.

- Design a strategy for hardening client operating systems.
- Design a strategy for restricting user access to operating system features.

Lecture Focus Questions:

- How can structuring Active Directory appropriately help you in managing workstation security?
- What is the difference between security templates and administrative templates?
- What type of software is controlled through an Internet Zone rule?
- What type of software restriction rule can you use to allow running all internally-developed scripts (while preventing running all other scripts)?
- How can physical security increase the security of client workstations beyond what is available within the operating system and through Group Policy?

Time

About 5 minutes