

## 2830 - Designing Security for Microsoft Networks

Duration: 3 Days

This three-day instructor-led course provides you with the knowledge and skills to design a secure network infrastructure. Topics include assembling the design team, modeling threats, and analyzing security risks in order to meet business requirements for securing computers in a networked environment. The course encourages decision-making skills through real-life scenarios that the target audience may encounter. You are given the task of collecting the information and sorting through the details to resolve the given security requirement.

### Course objectives:

After completing this course, students will be able to:

- Plan a framework for network security.
- Identify threats to network security.
- Analyze security risks.
- Design security for physical resources.
- Design security for computers.
- Design security for accounts and services.
- Design security for authentication.
- Design security for data.
- Design security for data transmission.
- Design security for network perimeters.
- Design an incident response procedure.

In addition, this course contains three teachable appendices that cover:

- Designing an acceptable use policy.
- Designing policies for managing networks.
- Designing an operations framework for managing security.

**Prerequisites:** This course requires that students meet the following prerequisites:

- A strong familiarity with Windows Server 2003 core technologies, such as those covered in Microsoft Official Curriculum (MOC) Course 2273: Managing and Maintaining a Microsoft Windows Server 2003 Environment.
- A strong familiarity with Windows Server 2003 networking technologies and implementation, such as those covered in:
  - MOC Course 2276: Implementing a Microsoft Windows Server 2003 Network Infrastructure: Network Hosts, and
  - MOC Course 2277: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure: Network Services, and
  - MOC Course 2278: Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure.
- A strong familiarity with Windows Server 2003 directory services technologies and implementation, such as those covered in MOC Course 2279: Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure.

**Audience:** This course is intended for IT systems engineers and security specialists who are responsible for establishing security policies and procedures for an organization. Students should have one to three years of experience designing related business solutions.

### **Module 1: Introduction to Designing Security**

A security design is a comprehensive plan that guides the implementation of security policies and procedures for an organization. A security design helps an organization to organize its assets to implement security in a consistent and effective manner.

This module describes the basic framework for designing network security and introduces key concepts used throughout the course. It also introduces a fictional organization which the labs in the course use as an ongoing case study.

#### **Lessons**

- Introduction to Designing Security for Microsoft Networks
- Contoso Pharmaceuticals: A Case Study

After completing this module, students will be able to:

- Provide an overview of designing security for Microsoft networks.
- Describe the components of the case study for this course.

### **Module 2: Creating a Plan for Network Security**

Plans for network security include documented security policies and procedures. These policies and procedures, when implemented, help to secure networks against compromises. This module describes the importance of security policies and procedures in a security design, and explains how a security design team must include representation from various members of the organization. The module also introduces the Microsoft Solutions Framework (MSF) process model, which provides a comprehensive framework that can be used to create a security design.

#### **Lessons**

- Introduction to Security Policies
- Designing Security by Using a Framework
- Creating a Security Design Team

#### ***Lab 2: Creating a Plan for Network Security***

- Exercise 1: Identifying Reasons Why Security Policies Fail
- Exercise 2: Determining the Members of a Security Design Team

After completing this module, students will be able to:

- Describe common elements of security policies and procedures.
- Create a security design framework by using the MSF process model.
- Create a security design team.

### **Module 3: Identifying Threats to Network Security**

Without security measures and controls in place, your data may be subjected to an attack. Some attacks are passive, which means that information is monitored; others are active, which means that the information is altered with intent to corrupt or destroy the data or the network itself.

Your networks and data are vulnerable to any of these types of attacks if you do not have a security plan in place.

In this module, you will learn how to identify possible threats to a network and understand common motivations of attackers. The module introduces the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) threat model as an effective way to predict where threats may occur in an organization.

#### **Lessons**

- Introduction to Security Threats
- Predicting Threats to Security

#### ***Lab 3: Identifying Threats to Network Security***

- Exercise 1: Identifying and Categorizing Threats by Using a Threat Model
- Exercise 2: Documenting Security Threats

After completing this module, students will be able to:

- Explain common network vulnerabilities and how attackers can exploit them.
- Predict threats to security by using a threat model.

### **Module 4: Analyzing Security Risks**

Many organizations cannot react to new security threats before their business is affected. Managing the security of their infrastructures—and the business value that those infrastructures deliver—has become a primary concern for information technology (IT) departments.

The Microsoft approach to security risk management is proactive and can assist organizations of all sizes with their response to the requirements presented by these environmental and legal challenges. A formal security risk management process enables enterprises to operate in the most cost-efficient manner by adopting a known and acceptable level of business risk. It also gives organizations a consistent, clear path to organize and prioritize limited resources in order to manage risk.

In this module, you will learn how to determine what resources in your organization require protection and how to prioritize those resources based on their value. You will then develop a risk management plan, based on the MOF risk model, to identify and analyze risks proactively and to determine an appropriate level of protection for each resource.

#### **Lessons**

- Introduction to Risk Management
- Creating a Risk Management Plan

#### ***Lab 4: Analyzing Security Risks***

- Exercise 1: Applying Quantitative and Qualitative Risk Analysis

After completing this module, students will be able to:

- Explain the purpose and operation of risk management.
- Create a risk management plan.

### **Module 5: Designing Physical Security for Network Resources**

Physical security refers to physical measures designed to safeguard personnel, property, and information. The term applies to architectural features such as location, layout, barriers, doors, locks and bolts, and lighting, but also includes measures such as access control systems, alarm systems, and CCTV systems.

In this module, you will determine threats and analyze physical risks to resources in an organization. You will then learn how to design security for facilities, computers, mobile devices, and hardware. You will also learn about implementing disaster recovery as a way to protect physical resources. This module focuses on physical access to resources and how to protect them. Other modules will focus on access to data and how to protect it.

#### **Lessons**

- Creating a Plan for Physical Security
- Creating a Design for Physical Security of Network Resources

#### **Lab 5: Designing Physical Security for Network Resources**

- Exercise 1: Identifying Potential Physical Vulnerabilities
- Exercise 2: Implementing Countermeasures

After completing this module, students will be able to:

- Create a plan for physical security.
- Create a design for physical security of network resources.

### **Module 6: Designing Security for Network Hosts**

The Windows Server 2003, Windows XP Professional, and Windows Vista operating systems provide many features and capabilities that you can use to configure and maintain a secure network operating environment. In fact, there are security capabilities in nearly every area of Windows. Many of these security features and capabilities have been added or enhanced since the introduction of the Microsoft Windows 2000 Professional and Windows 2000 Server operating systems.

In this module, you will learn how to determine threats and analyze risks to network hosts in an organization. You will also learn how to design security for network hosts throughout their life cycles, from initial purchase to decommissioning.

#### **Lessons**

- Creating a Security Plan for Network Hosts
- Creating a Design for the Security of Network Hosts

#### **Lab 6: Designing Security for Network Hosts**

- Exercise 1: Identifying Vulnerabilities When Applying Security Updates
- Exercise 2: Identifying Vulnerabilities When Decommissioning Computers

After completing this module, students will be able to:

- Create a security plan for network hosts.
- Create a design for the security of network hosts.

### **Module 7: Designing Security for Accounts and Services**

Computer networks use accounts to grant users, applications, and network services access to the information on a network. Network services are server applications that are usually hosted on dedicated server computers.

If an attacker gains access to an account that has excessive privileges, or breaks the password that is associated with an account, the attacker can obtain authorized access to a network.

Windows services are executable programs that run in sessions outside the session that the user who is currently logged on is using. In this way, services run in the background, independent of any user session. Services can start automatically when the computer starts, and can also be paused and restarted. Services may not show a user interface, although they typically communicate with a user interface to control and administer the service. Because of this behavior, services are ideal for use on a server or whenever you require long-term functionality that does not interfere with other users who are working on the same computer. In addition to services that Microsoft has created, many third-party vendors design products to be deployed as services running continuously in the background. Antivirus services are an example of this type of product. In this module, you will learn how to determine threats and analyze risks to accounts and services in an organization. You will also learn how to design security for accounts and services, including determining security requirements, creating policies, and designing strategies to manage security.

#### **Lessons**

- Creating a Security Plan for Accounts
- Creating a Security Plan for Services
- Creating a Design for Security of Accounts and Services

#### **Lab 7: Designing Security for Accounts and Services**

- Exercise 1: Identifying Potential Account Vulnerabilities
- Exercise 2: Applying Countermeasures

After completing this module, students will be able to:

- Create a security plan for accounts.
- Create a security plan for services.
- Create a design for security of accounts and services.

### **Module 8: Designing Security for Authentication**

In this module, you will learn how to determine threats and analyze risks to authentication. You will learn how to design security for authenticating local users, remote users, and users who access your network across the Internet. You will also learn when to choose multifactor authentication for additional security.

#### **Lessons**

- Creating a Security Plan for Authentication
- Creating a Design for Security of Authentication

#### **Lab 8: Designing Security for Authentication**

- Exercise 1: Identifying Potential Authentication Vulnerabilities
- Exercise 2: Applying Countermeasures

After completing this module, students will be able to:

- Create a security plan for authentication.
- Create a design for security of authentication.

### **Module 9: Designing Security for Data**

Business data is one of the most valuable resources in many organizations. If data were to be irreparably damaged, lost, or exposed to competitors, many organizations would be adversely affected and perhaps even driven out of business. For client hosts, protecting data can be particularly daunting because portable computers can be stolen from mobile users, and backing up data for mobile users is very difficult. Protecting data that is stored on servers is still a significant challenge, but for most organizations it is one that is achievable. For these reasons, many companies require their end users to store their critical data on servers managed by their information technology (IT) department. Data can be protected through the use of access control lists (ACLs) on files and folders, by using encryption, and by using an effective backup and restore strategy.

In this module, you will learn how to determine threats and analyze risks to data in an organization. You will learn how to design an access control model for files and folders in order to protect data that is stored on network servers. You will also learn about considerations for encrypting and managing data.

#### **Lessons**

- Creating a Security Plan for Data
- Creating a Design for Security of Data

### **Lab 9: Designing Security for Data**

- Exercise 1: Identifying Potential Data Vulnerabilities
- Exercise 2: Designing Countermeasures

After completing this module, students will be able to:

- Create a security plan for data.
- Create a design for security of data.

### **Module 10: Designing Security for Data Transmission**

In this module, you will learn how to determine threats and analyze risks to data transmission in an organization. You will also learn how to design security for various types of data transmission, including traffic on local area networks (LANs), wide area networks (WANs), Virtual Private Networks (VPNs), wireless networks, and the Internet.

#### **Lessons**

- Creating a Security Plan for Data Transmission
- Creating a Design for Security of Data Transmission

### **Lab 10: Designing Security for Data**

- Exercise 1: Identifying Potential Data Transmission Vulnerabilities
- Exercise 2: Implementing Countermeasures

After completing this module, students will be able to:

- Create a security plan for data transmission.
- Create a design for security of data transmission.

### **Module 11: Designing Security for Network Perimeters**

Properly configured firewalls and border routers are the cornerstone of perimeter security. However, all of these devices must be properly secured because the entire network is put at risk when any one of them is compromised. Organizations must therefore invest time and resources in securing not only the Virtual Private Network (VPN) servers and the remote access servers (RAS), but also the mobile computers that are used to connect to those servers. To do business on and through the Internet, organizations must make some of their business applications and data accessible through the Internet. Traditional packet-filtering firewalls block network ports and computer addresses, but ports must be opened for the business applications. This means that your organization requires firewalls or proxy servers that are application-aware and capable of filtering network traffic at the application layer.

In this module, you will learn how to determine threats and analyze risks to network perimeters. You will also learn how to design security for network perimeters, including perimeter networks (also known as DMZs, demilitarized zones, and screened subnets), and for computers that connect directly to the Internet.

#### **Lessons**

- Creating a Security Plan for the Perimeter of a Network
- Creating a Design for Security of Network Perimeters

### **Lab 11: Designing Security Network Perimeters**

- Exercise 1: Identifying Potential Perimeter Network Vulnerabilities
- Exercise 2: Implementing Countermeasures

After completing this module, students will be able to:

- Create a security plan for the perimeter of a network.
- Create a design for security of network perimeters.

## **Module 12: Responding to Security Incidents**

Network security for an organization is an exercise in prevention. A good security design that is properly implemented will prevent most of the most common attacks. However, it is very likely that an attacker will eventually penetrate the defenses that you design.

When an attack happens, the key to limiting damage is early detection and a rapid and orderly response. Auditing is an important tool to help you to detect network abnormalities that may indicate attacks. An incident response procedure is a series of steps that you design in advance to guide your organization during a security incident.

### **Lessons**

- Introduction to Auditing and Incident Response
- Designing an Audit Policy
- Designing and Incident Response Procedure

### ***Lab 12: Responding to Security Incidents***

- Exercise 1: Identifying Potential Vulnerabilities
- Exercise 2: Implementing an Incident Response Team
- Exercise 3: Implementing an Incident Response Plan

After completing this module, students will be able to:

- Describe auditing and incident response.
- Design an audit policy.
- Design an incident response procedure.