This course of study outlines the sequence of learning activities to help you develop competence in the subject area of TSV2. Your competence will be assessed as you complete the assessment MCSE Server 2003 Exam 70-298 (TSV2). This course of study may take up to nine weeks to complete depending on your educational background, work experience, and the time you are able to dedicate to your studies. Consult with your mentor if you wish to accelerate your progress through this course of study. It is important that you follow the activities sequentially as you prepare for your assessment. This tool is also designed to help you become an independent learner by providing multiple learning methods.

Introduction

Are you currently an information technology professional? Are you planning to become an information technology professional in the future? Or perhaps you simply want to become an expert in the Windows Server 2003 operating system? The Designing Security for a Microsoft Server 2003 Network (TSV2) Course of Study provides you the opportunity to learn and master the security domain of Windows Server 2003.

Indeed, Microsoft Windows Server 2003 is one of the most widely used Windows server operating systems in industries today. This operating system provides robust functions of computing that no other previous Windows Server operating system (e.g., Windows NT Server 4.0, Windows 2000 Server/Advance Server) has ever provided. Successfully mastering Windows Server 2003 provides a number of benefits, including the opportunity to become an expert in the field of information technology and the ability to improve productivity through the installation, configuration, and troubleshooting of computers running the server operating system as well as planning, implementing, troubleshooting, and maintaining a Microsoft Windows Server 2003 network environment.

If you have experience with previous Microsoft server operating systems, including Windows NT Server 4.0 or Windows 2000 Servers/Advance Servers, it will be relatively easy for you to master Windows Server 2003, as it inherits many attributes from those previous operating systems. According to this course of study, the total estimated time needed for studying and getting prepared for the MCSE Server 2003 Exam 70-298 (TSV2) is about nine weeks. Confidence, dedication, diligence, and perseverance are the key ingredients for you to successfully pass the TSV2 assessment.

Once you successfully pass your MCSE Server 2003 Exam 70-298, you will become a Microsoft Certified Professional (MCP)-a recipient of a highly-reputable professional certification in the field of information technology. This certificate not only represents your achievement in successfully mastering Windows Server 2003 security but it also serves as a stepping stone for you to enter the information technology (IT) industry if you are not currently an IT professional. If you are currently an IT professional, this certificate may potentially help you obtain a promotion by your current employer or even an increase in your salary. Most important of all, it will help you become more successful in your lifelong career.

This course of study will serve as an effective tool in helping you successfully command the
Windows Server 2003 operating system. It will also help you pass your MCSE Server 2003 Exam 70-298 the first time you take it at a Prometric testing center. Please follow the outlined activities so that you can maximize your learning outcomes.

There are four competencies covered by this course of study:

Competency: Prevention, Detection, Isolation, and Recovery
The graduate can design a framework for implementing security using prevention, detection, isolation, and recovery.

Competency: Technical Constraints
The graduate can analyze technical constraints in designing security.

Competency: Access Control Strategy
The graduate can design an access control strategy for data.

Competency: Client Infrastructure Security
The graduate can create the physical design for client infrastructure security.

The textbook chapters assigned in this course cover each of these competencies and the competencies covered by the MCSE Server 2003 Exam 70-298 (TSV2) assessment.

Note: Microsoft refers to the competencies as "skills being measured."

The assessment is composed of 55 questions (randomly selected from a pool of questions) and must be completed between one and three hours. To pass the assessment, you must achieve a score of at least 700 out of 1000 total points. Once you submit proof of your passing score (i.e., scan and e-mail, fax, or mail your score report to WGU), WGU will record your result in your AAP.

Required Learning Resources:


ExamForce: 70-298 Designing Security for a Microsoft Windows Server 2003 Network

IT Academy e-Learning content for TSV2: Course 2830 and lab: Designing Security for Microsoft Networks
Preparing for Success

To successfully complete the TSV2 assessment, you need the appropriate resources to aid your learning. You should also prepare a calendar to schedule time devoted to your studies. Share your calendar with family and friends so that they are aware of your obligations.

Topics

Acquire Learning Resources

Arrange to obtain the learning resources listed below so there will be no delays in your studies. These items are essential for you, as this document will guide you in the use of these materials. Some of these items must be shipped to you, so be sure that your mailing address information is current. If you click your name on your AAP, you can check your contact information.

Resources

Obtain Your Textbook
URL: http://wgu.skillport.com

The textbook used for TSV2 is:


It is the required learning resource for Security II (TSV2).

All required readings for TSV2, including the textbook, are available online at SkillSoft free for you to access whenever you need them. Please follow this course of study and complete the required readings, hands-on practices, and questions and answers accordingly.

If you wish to purchase a hard copy of the textbook, you may also choose to buy a hard copy from the WGU Bookstore or another bookstore at your own cost. Please use the ISBN number(s) to make sure that you order the correct edition.

Access SkillSoft Modules
URL: http://wgu.skillport.com

Make sure that you can access your SkillSoft account, since there is a Windows Server 2003 installation review that you will need to work through during this course of study. You will follow the same log-in procedure to log in to WGU's SkillPort portal as you did to access your textbook. Keep in mind that WGU students are batch-loaded into the SkillSoft site at the end of each week.
If you have not met AAV, you may need to wait until the following week to gain access.

You will need to do the following in order to access this library:

Access the SkillSoft site

Enter your WGU portal username and original WGU password.

If you cannot remember your original WGU password, you can go to the "Forgot your Password?" link on the page (near the bottom) and enter your WGU portal user ID, and a new password will be sent to your my.wgu.edu e-mail address.

If you have any difficulty with your account or signing on, please contact the Learning Resource Department at learning@wgu.edu or 801-993-1334 for assistance.

**Familiarize Yourself With ExamForce**
ExamForce is a powerful tool; you will use it for review and final preparation. Enroll for this resource through your AAP.

Get familiar with how ExamForce works. It has three modes, which progress in a logical sequence:

The pretest mode is a diagnostic mode to find the remaining holes in your learning.

The adaptive drill mode helps you hone competence by repetitive drills for review. This mode includes a maintenance aspect to ensure you do not forget what you already know. The adaptive drill mode fills in holes.

The simulated exam mode simulates the real exam to keep you sharp.

You will use ExamForce in the final weeks of this course of study as you prepare for the OFV1 assessment.

**Access IT Academy**
URL: http://itacademy.microsoftlearning.com

Access the Microsoft e-learning content for TSV2 through the IT Academy website. Enter the access code in the text field and confirm that you have read the license agreement. The access code for the TSV2 e-learning content: 7049-09W298-7212

You will need to sign in with a Windows Live ID. If you have a MSN Hotmail, MSN Messenger, or
Passport account, this is your Windows Live ID. If you do not already have one of these types of accounts, follow the instructions to sign up with a free Windows Live ID.

When you have logged in you will see your e-learning content, which you will complete in an upcoming activity:

Course 2830 and lab: Designing Security for Microsoft Networks

Prepare for Your Studies

You need to also make sure that you have the right setup of computer equipment and software to get started. You need to be able to access the online message board that supports this course of study, and you need to know where to go to get help should you need additional support with your learning.

Resources

Hands-On Labs
It is highly recommended that you have a spare computer with Windows Server 2003 installed for hands-on practice purposes. The hands-on labs are incorporated throughout your textbook, MCSA/MCSE Self-Paced Training Kit (Exam 70-298). Each chapter of the book provides a "troubleshooting lab." These labs are designed to help you roll up your sleeves and dive into the content. Many of these labs will have you looking at settings on your home computer and often making changes to them. Be sure you are careful to back up your settings before making any changes to your system.

You can conduct hands-on practice in the following ways:

You can use your current PC or laptop that runs Windows Server 2003 and do the hands-on practices in this course of study. It is highly recommended that you back up your data on a daily basis in case your PC or laptop malfunctions due to configurations made during those hands-on practices. You should also have your CD of Windows Server 2003 (not the 180-day trial version) handy in case you need to reinstall Windows Server 2003 Professional on your PC or laptop.

Note: Did you know that as a student at WGU you qualify for free Microsoft software related to your degree program? You can learn more about this program by visiting the message board.

Another alternative is to have a spare PC or laptop ready, if available, so that you can conduct the hands-on practices after installing the 180-day trial version of Windows Server 2003. This option is most favorable, as you do not have to worry about losing your data and time.

Finally, you can consider partitioning your current PC or laptop if it is running Windows NT/2000/XP/VISTA and if you have the software to help you partition your current hard drive on your computer. This option saves you from buying additional hardware (i.e., PC, laptop, hard
drive) in order to conduct hands-on practices in this course of study. Please note that you still need to back up your data on a daily basis. This option does permit you to install the 180-day trial version on your current PC or laptop running the Windows NT/2000/XP/VISTA operating system(s).

**Participate and Contribute to the Message Board**
In the lower right-hand corner of the course of study screen there is a message board area. Throughout your studies, you will want to follow the questions, observations, and responses of the other students and the expert advice of the course mentor. If you have questions of your own, do not hesitate to use this resource to get those answered as you develop your competencies.

**Obtain a Notebook or Digital Journal**
As you engage with the activities throughout this course of study, you will be answering questions, completing exercises, sketching out concepts, and so forth. Taking these notes in a study journal (either on paper or electronically) makes your learning more active. It also provides an excellent source of important materials to review prior to demonstrating your competencies through the TSV2 assessment.

**Getting Help With Your Learning**
As you move through the textbook, you are strongly encouraged to complete the questions at the end of each chapter. If you have difficulty in answering questions or completing any of the tasks in each activity with confidence, it is recommended that you try one or more of the following:

Look in the message boards to see if you can find similar questions posed by others.

Reach out to your peers for assistance, if possible.

Contact your course mentor directly for help. The mentor's contact information is available in the upper-right corner of the course of study screen.
Creating the Conceptual Design for Network Infrastructure Security by Gathering and Analyzing Business and Technical Requirements

This section provides an overview of the skills necessary for planning, designing, and implementing a structure for network security within a Microsoft Server 2003 environment.

By understanding the fundamental concepts of planning, designing, and implementing the conceptual design for network infrastructure security, you will be able to analyze business requirements for designing security, design a framework for designing and implementing security, and analyze technical constraints when designing security for both wired and wireless business environments. In addition, you will learn how to configure Microsoft Internet Information Services (IIS) settings.

Properly designed security frameworks can make or break a business. The only way to be successful at designing a solid security framework is to be familiar with the business model of the organization, the technical infrastructure, and of course the already-existing security policies. This section will give you the foundation you need to ultimately design a framework that you will learn how to perform security against.

Topics

Creating the Conceptual Design for Network Infrastructure Security

This topic is associated with chapter 1 ("Creating a Conceptual Design for Network Infrastructure Security") of the MCSA/MCSE Self-Paced Training Kit (Exam 70-298) textbook. This topic focuses on the basic concepts associated with creating the conceptual design for network infrastructure security. Specifically, this section discusses the knowledge and skills necessary for analyzing business requirements for designing security, including the considerations of existing policies and procedures, the sensitivity of data, the cost, the legal requirements, the end-user impact, the interoperability, the maintainability, the scalability, and the risks.

This topic provides insight into the skills necessary for analyzing the organizational requirements of different types of data, analyzing the risks to security within the current IT administration structure and security practices, designing a framework for designing and implementing security, predicting threats to the network from internal and external sources, designing a process for responding to incidents, designing segmented networks, designing a process for recovering services, identifying capabilities of the existing infrastructure, and identifying technology limitations.

Resources

Analyzing Business Requirements for Information Security

In chapter 1 of the textbook, read lesson 1 (pp. 1.5-1.22) and then complete the associated hands-on practices at the end of lesson 1. Consider the following questions as you work through the lesson:
What is the purpose of analyzing business requirements?

How do you incorporate common business drivers into security design?

How do maintainability issues pose a threat to security?

In what way can you analyze exiting security policy and procedures?

How can you possibly categorize and secure data based on an organization’s needs?

In what way should you analyze risks to security in the existing IT administration structure?

Complete the following hands-on practices before moving to the next lesson:

Hands-On Exercise 1: Analyzing Business Requirements (p. 1.24)

Hands-On Exercise 2: Evaluating the Current Security System Policy (p. 1.26)

Hands-On Exercise 3: Placing Documents in Data Categories (p. 1.27)

Hands-On Exercise 4: Identifying Noncompliant Security Policies (p. 1.27)

Hands-On Exercise 5: Deciding How to Secure Public Access to a Company Website (p. 1.28)

Creating the Security Design Framework

In chapter 1 of the textbook, read lesson 2 (pp. 1.29-1.42) and then complete the associated hands-on practices at the end of lesson 2. Consider the following questions as you work through the lesson:

What are the components of a security design framework?

What is the process for creating a security design framework?

What are the principles of information security design?

What can the threat modeling do?

How will you design a process for responding to incidents?

What elements should you consider when designing the use of segmented networks?

How should you design a process for recovering services?
Complete the following hands-on practices before moving to the next lesson:

Hands-On Exercise 1: Creating the Security Design Framework-Predicting Threats to a Company (p. 1.45)


Hands-On Exercise 5: Creating the Security Design Framework-Identifying Devices that Segment Internal Networks Into Zones of Trust (p. 1.49)

Analyzing Technical Constraints That Affect Security Design
In chapter 1 of the textbook, read lesson 3 (pp. 1.50-1.52) and then complete the associated hands-on practices at the end of lesson 3. Consider the following questions as you work through the lesson:

How should you identify capabilities of legacy infrastructure and integrate them into the design?
What are the technology limitations?
Do you have skills in analyzing interoperability constraints?

Complete the following hands-on practices before moving to the next lesson:


Chapter 1 Additional Activities
Complete the following:

Design Activity: Developing a List of Security Issues (p. 1.55)

Questions and Answers (p. 1.59)

**IT Academy E-Learning**
URL: http://itacademy.microusoftelearning.com

Access the Microsoft e-learning content for TSV2 through the IT Academy website. Begin working through the course materials and lab for "Course 2830: Designing Security for Microsoft Networks." As you move through the COS, continue to progress through this course.

This resource was created by Microsoft and will help you prepare for your Microsoft certification exam.

**Designing Security for Wireless Networks**

This topic is associated with chapter 12 ("Designing Security for Wireless Networks") of the MCSA/MCSE Self-Paced Training Kit (Exam 70-298) textbook. This topic focuses on the skills needed for designing public and private wireless LAN with security and for designing 802.1x authentications for wireless networks.

**Resources**

**Designing Security for Wireless Networks**

In chapter 12 of the textbook, read lesson 1 (pp. 12.3-12.15) and then complete the associated hands-on practice at the end of lesson 1. Consider the following questions as you work through the lesson:

What is the purpose of an 802.11 wireless network?

What are the secure and insecure wireless network topology options?

What are the wireless network security features?

What processes and procedures are involved when designing security for wireless networks?

What kinds of threats can wireless networks introduce?

How should you design security for 802.1b wireless networks?
What elements should you consider when designing security for 801.11i (WPA) networks?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Securing a Rogue Access Point (p. 12.16)

Designing Security Using 802.1x for Wireless Networks
In chapter 12 of the textbook, read lesson 2 (pp. 12.3-12.32) and then complete the associated hands-on practice at the end of lesson 2. Consider the following questions as you work through the lesson:

How can you improve 802.1x wireless security?
What are the infrastructure requirements of 802.1x?
How do 802.1x networks authenticate?
What elements should you include when designing security using 802.1x?
How can you design authentication using 802.1x?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Selecting Authentication Protocols (p. 12.32)

Chapter 12 Additional Activities
Complete the following:

Design Activity: Securing a Network from a Free WirelessAccess Site (p. 12.33)
Questions and Answers (p. 12.39)

Chapter 12 Additional Review
SkillSoft provides an excellent way to review the Windows XP installation areas you may have struggled with in the textbook.

This course module is located in the "My Plan" area of your SkillSoft account. Navigate to "My Plan" > "IT Undergraduate" > "TSV2" > "70-298: Designing Security for a Microsoft Windows Sever 2003 Network." Start and review the "Creating a Conceptual Design for Network Infrastructure" lesson.


Remember, if you are feeling confused after completing all the activities for this topic area, please visit the message board or contact the course mentor directly.
Creating the Conceptual Design for Network Infrastructure Security by Gathering and Analyzing Business and Technical Requirements (Continued)

This section is a continuation of the previous section. As was mentioned previously, this section provides an overview of the skills necessary for planning, designing, and implementing a structure for network security within a Microsoft Server 2003 environment.

By understanding the fundamental concepts of planning, designing, and implementing the conceptual design for network infrastructure security, you will be able to analyze business requirements for designing security, designing a framework for designing and implementing security, and analyzing technical constraints when designing security for both wired and wireless business environments. In addition, you will learn how to configure Microsoft Internet Information Services (IIS) settings.

This section is a bit different than the last as it focuses on hardening and protection for IIS and web-based applications. Learning to design IIS security baselines and user authentication for IIS will help you protect your web server from malicious hackers and disgruntled employees.

Topics

Designing Security for IIS

This topic is associated with chapter 13 ("Designing Security for IIS") of the MCSA/MCSE Self-Paced Training Kit (Exam 70-298) textbook. This topic focuses on the skills needed for designing security for Microsoft Internet Information Services (IIS).

Resources

Designing the IIS Security Baselines
In chapter 13 of the textbook, read lesson 1 (pp. 13.3-13.27) and then complete the associated hands-on practice at the end of lesson 1. Consider the following questions as you work through the lesson:

How should you design security for IIS?

What are the viable ways to reduce the web servers, websites, applications, and server resources?

How can data in transit be protected?

What major considerations should be included when designing a secure content management strategy?

How can you design monitoring and maintenance strategies for IIS?
In what way can you design access control for databases on the web server?

What is an effective way to configure web servers to isolate websites and applications?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Designing IIS Security to Meet Business Needs (p. 13.31)

**Designing User Authentication for IIS**

In chapter 13 of the textbook, read lesson 2 (pp. 13.32-13.42) and then complete the associated hands-on practice at the end of lesson 2. Consider the following questions as you work through the lesson:

How should you design user authentication for IIS?

How do you integrate authentication for websites and servers?

What are the IIS authentication methods?

How can you integrate certificates when designing IIS user authentication?

What is the process of designing authentication using Remote Authentication Dial In User Service (RADIUS)?

What are the possible options that are available when designing authentication for File Transfer Protocol (FTP)?

What elements should be considered when designing authentication for Simple Mail Transfer Protocol (SMTP)?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Selecting Authentication Methods for IIS (p. 13.42)

**Chapter 13 Additional Activities**

Complete the following:
Note: It is a good idea to record your responses in your notebook; this way, you will be able to review quickly as you prepare to take the actual assessment.
Creating the Logical Design for Network Infrastructure Security

This section provides an overview of the process and procedures of designing the logical infrastructure and network infrastructure for physical security.

By understanding the fundamental concepts of designing the logical infrastructure for network security, you will be able to design a Public Key Infrastructure (PKI), Certificate Authority (CA) hierarchy implementation, and enrollment and distribution process; and establish renewal, revocation, and auditing processes.

Topics

Designing the Logical Infrastructure

This topic is associated with chapter 2 ("Designing the Logical Infrastructure") of the MCSA/MCSE Self-Paced Training Kit (Exam 70-298) textbook. This topic focuses on the skills needed for designing the logical infrastructure necessary for protecting network resources during the exchange of data via the Internet.

Resources

Building a Logical Security Infrastructure by Using Certificate Services

In chapter 2 of the textbook, read lesson 1 (pp. 2.5-2.8) and then complete the associated hands-on practice at the end of lesson 1. Consider the following questions as you work through the lesson:

What exactly are the pillars of information security?

How can you integrate the pillars of information security in your designs?

In what way can you build a logical security information infrastructure by using certificate services?

What are the proper ways to identify the components of a public key infrastructure?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Using Certificates for Authentication and Authorization (p. 2.12)
Designing a CA Hierarchy
In chapter 2 of the textbook, read lesson 2 (pp. 2.15-2.30) and then complete the associated hands-on practice at the end of lesson 2. Consider the following questions as you work through the lesson:

How does a CA hierarchy work?
What are the effective ways to protect the root CA hierarchy infrastructure?
How should you install an offline root CA?
What are the different types of CA hierarchies?
What are the effective ways to design different types of CA hierarchies?
What is the certificate chaining process?
Why do you need qualified subordination?
In what ways can you secure CAs?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Designing a CA Hierarchy (p. 2.31)

Designing the Certificate Enrollment Process
In chapter 2 of the textbook, read lesson 3 (pp. 2.35-2.43) and then complete the associated hands-on practice at the end of lesson 3. Consider the following questions as you work through the lesson:

What is the exact certificate enrollment process?
What should be taken into account when designing certificate enrollment?
What is the proper way to design the certificate enrollment and distribution policy?
In which manner should you configure enrollment and certificate distribution for the offline root CA?
Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Designing the Certificate Enrollment Policy (p. 2.46)

**Designing the Renewal, Revocation, and Auditing Processes**
In chapter 2 of the textbook, read lesson 4 (pp. 2.50-2.60) and then complete the associated hands-on practice at the end of lesson 4. Consider the following questions as you work through the lesson:

What are renewal, revocation, and auditing?
What are the guidelines for designing the renewal policy?
How does the revocation process work?
How does a delta certificate revocation list (CRL) work?
What are the key elements that should be considered when designing the revocation process?
How should you design a revocation policy?
What should be taken into account when designing the auditing process?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Designing a CRL Location and Publication Periods (p. 2.63)

**Designing Security for the Certificate Authority**
In chapter 2 of the textbook, read lesson 5 (pp. 2.65-2.70) and then complete the associated hands-on practice at the end of lesson 5. Consider the following questions as you work through the lesson:

What are the available CA-specific administration roles and operating system roles?
How can you use CA administration roles?
What can an operating administrator do to enable CA role separation?
What are the proper procedures if you want to design additional security for CA services?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Designing CA Administrative Roles (p. 2.71)

**Chapter 2 Additional Activities**
Complete the following:

Design Activity: Designing the Logical Infrastructure (p. 2.73)

Questions and Answers (p. 2.78)
Creating the Physical Design for Network Infrastructure Security (Part I)

This section provides an overview of how to create the physical design for network infrastructure security within a Windows Server 2003 network environment.

By understanding the fundamental concepts of planning, designing, and implementing the physical design for the network infrastructure security, you will be able to design network security infrastructure, specify the required protocols for the firewall configuration, design Internet Protocol Security (IPSec) policy, secure Domain Name System (DNS) implementation, manage risks, design security for emergency management services, and design a security update infrastructure.

Topics

Designing the Network Infrastructure for Physical Security

This topic is associated with chapter 3 ("Designing the Network Infrastructure for Physical Security") of the MCSA/MCSE Self-Paced Training Kit (Exam 70-298) textbook. This topic introduces skills necessary for creating the physical design for a secure network infrastructure, including designing for network infrastructure security, specifying the required protocols for the firewall configuration, designing Internet protocol filtering, designing Internet Protocol Security (IPSec) policy, securing DNS implementation, and designing security for data transmission.

Resources

Designing Network Border Control
In chapter 3 of the textbook, read lesson 1 (pp. 3.3-3.19) and then complete the associated hands-on practice at the end of lesson 1. Consider the following questions as you work through the lesson:

What is exactly the process of designing network border control?

What are the common categories of data?

How can you determine resource needs?

In what ways can you classify data?

What is logical infrastructure support?

If you want to design network segments for security, where should you start?

What are the proper ways for you to design effective border controls?

What should be considered when choosing border controls?
If you want to select and use effective border controls, how can you accomplish this goal?

Why should you design Active Directory replication over firewalls?

How should you secure Active Directory traffic?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Designing Network Border Controls (p. 3.22)

**Securing DNS**
In chapter 3 of the textbook, read lesson 2 (pp. 3.27-3.29) and then complete the associated hands-on practice at the end of lesson 2. Consider the following questions as you work through the lesson:

How is DNS integrated into an Active Directory network?

What are some of the common attacks on DNS?

What are the methods for securing DNS deployments in face of common attacks on DNS?

Which measure should you take in order to secure DNS zone replication?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Securing DNS (p. 3.31)

**Designing Security for Internal Data Transmission**
In chapter 3 of the textbook, read lesson 3 (pp. 3.34-3.50) and then complete the associated hands-on practice at the end of lesson 3. Consider the following questions as you work through the lesson:

What are the criteria to select methods to secure data transmission?
How can you possibly create Internet protocol filters?

Under what conditions can you create a negotiating IPSec policy?

Why does the IPSec startup protect?

How would you design IPSec startup protection?

How would you acquire knowledge and skills necessary for designing an IPSec negotiation policy?

Why do you need to select and configure negotiation policies?

What are the considerations behind the guidelines for overall IPSec policy design?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Designing an IPSec Policy (p. 3.52)

**Chapter 3 Additional Activities**

Complete the following:

Design Activity: Designing the Network Infrastructure for Physical Security Scenario (p. 3.63)

Questions and Answers (p. 3.67)

**Designing Security for Network Management**

This topic is associated with chapter 4 (“Designing Security for Network Management”) of the MCSA/MCSE Self-Paced Training Kit (Exam 70-298) textbook. This topic focuses on the skills needed for managing risk, managing networks, designing administration of servers by using common administration tools, and designing security for emergency management services.

**Resources**

**Managing Administrative Risks**

In chapter 4 of the textbook, read lesson 1 (pp. 4.5-4.11) and then complete the associated hands-on practice at the end of lesson 1. Consider the following questions as you work through the lesson:
What is the process of managing administrative risks?

What are some of the common vulnerabilities in network management?

What are the differences between isolation and autonomy?

What is a security boundary?

What is the administrative security boundary?

What are the accepted practices in security installation?

What are the security considerations associated with automated deployments?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Documenting the Process of Creating a Secure Installation (p. 4.15)

**Designing Secure Administration Practices**
In chapter 4 of the textbook, read lesson 2 (pp. 4.17-4.24) and then complete the associated hands-on practice at the end of lesson 2. Consider the following questions as you work through the lesson:

What is the process for securing administration practices?

How can you reduce privilege group membership?

How can you protect administrative systems?

In which ways can you protect PDAs used for administration?

What are the proper ways to secure administrative channels?

Under what circumstances should you design the division of management duties?

Complete the following hands-on practice before moving to the next lesson:
Hands-On Exercise 1: Inspecting Administration Tools and Securing Their Use (p. 4.38)

Securing Emergency Management Services
In chapter 4 of the textbook, read lesson 3 (pp. 4.39-4.42) and then complete the associated hands-on practice at the end of lesson 3. Consider the following questions as you work through the lesson:

Why and when should you use Emergency Management Services (EMS)?
What exactly is out-of-band management?
What is an out-of-band infrastructure?
What are the components of EMS?
What are the guidelines for security EMS?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Securing EMS (p. 4.43)

Chapter 4 Additional Activities
Complete the following:

Design Activity: Designing Security for Network Management (p. 4.44)
Questions and Answers (p. 4.48)
Creating the Physical Design for Network Infrastructure Security (Part II)

This section is a continuation of the previous instruction. As was mentioned previously, this section provides an overview of how to create the physical design for network infrastructure security within a Windows Server 2003 network environment.

By understanding the fundamental concepts of planning, designing, and implementing the physical design for the network infrastructure security, you will be able to design network security infrastructure, specify the required protocols for the firewall configuration, design IPSec policy, secure DNS implementation, manage risks, design security for emergency management services, and design a security update infrastructure. In addition to what you were introduced to previously, you will learn that many successful computer attacks are the result of vulnerabilities with existing patches that were never installed. The textbook calls this phenomenon "configuration mitigation." The only way to protect against vulnerability attacks is to continually incorporate updated security information and security updates regularly.

Topics

Designing Security Update Infrastructure

This topic is associated with chapter 5 ("Designing a Security Update Infrastructure") of the MCSA/MCSE Self-Paced Training Kit (Exam 70-298) textbook. This topic focuses on the skills needed for designing a security update infrastructure, specifically in terms of designing a Software Update Services (SUS) infrastructure, designing group policy to deploy software updates, and designing a strategy for identifying computers that are not at the current patch level.

Resources

Introduction to Designing a Security Update Infrastructure

In chapter 5 of the textbook, read lesson 1 (pp. 5.3-5.17) and then complete the associated hands-on practice at the end of lesson 1. Consider the following questions as you work through the lesson:

Which key elements should you consider when designing a security update infrastructure?

Which are the changes that require security updates?

What are the common methods for updating systems?

How should you choose the best combination of update methods, if needed?

Where can you find the latest security vulnerability information?

Under what circumstances should you design a security update infrastructure?
Why do you need to apply SUS, and how does it work?

What are the recommended ways to secure the SUS server?

How can you use your current knowledge and skills to design a software update infrastructure by using SUS?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Documenting Business and Technical Constraints for the SUS Infrastructure Design (p. 5.25)

**Designing Client Configuration for the Security Update Infrastructure**
In chapter 5 of the textbook, read lesson 2 (pp. 5.27-5.31) and then complete the associated hands-on practice at the end of lesson 2. Consider the following questions as you work through the lesson:

What are the common practices if you want to configure SUS clients?

What are the policies in Group Policy that are recommended when configuring SUS client computers?

What are the user-specific settings used to solve SUS issues for users?

How can you modify the registry values when configuring SUS clients?

What is the proper way for you to design Group Policy management of SUS client operations?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Designing GPOs (p. 5.33)

**Monitoring and Improving the Security Patch Update Process**
In chapter 5 of the textbook, read lesson 3 (pp. 5.35-5.42) and then complete the associated hands-on practice at the end of lesson 3. Consider the following questions as you work through the lesson:
Why do you need to implement security patching programs?

What is the proper method for you to audit the security patching process?

How can the Microsoft Baseline Security Analyzer (MBSA) help you secure your network?

How does MBSA scan computers for missing patches?

What are the basic requirements for MBSA scanning?

What is the rationale for using MBSA to audit patch applications?

How do you determine patch status by using SUS and client logs?

How do you test security patches?

What are the best practices for you to monitor and improve the patch management process?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Considering the Implications of Using MBSA (p. 5.46)

Chapter 5 Additional Activities
Complete the following:

Design Activity: Designing a Security Update Infrastructure (p. 5.48)

Questions and Answers (p. 5.52)
Designing an Access Control Strategy for Data (Part I)

This section provides an overview of the skills needed for designing an access control strategy for data.

By understanding the fundamental concepts associated with designing access control for data, you will be able to design a logical authentication strategy, design secure communication between networks, design security by server role, and design access control for enterprise data.

You will also learn the importance of authentication strategies for a network. If unauthorized users can gain access to your network, they can navigate to wherever they want, accessing whatever they want, and potentially compromising data and protocols. Strong password policies, appropriate trust relationships, and securely-designed authentication protocols are appropriate steps toward controlling unauthorized access.

Topics

Designing a Logical Authentication Strategy

This topic is associated with chapter 6 ("Designing A Logical Authentication Strategy") of the MCSA/MCSE Self-Paced Training Kit (Exam 70-298) textbook. In this section, you will learn how to design forest and domain trust models, design security that meets interoperability requirements, and establish account and password requirements for security.

Resources

Designing Forest and Domain Trust Models

In chapter 6 of the textbook, read lesson 1 (pp. 6.5-6.20) and then complete the associated hands-on practice at the end of lesson 1. Consider the following questions as you work through the lesson:

What is the process for designing forest and domain trust models?
How do you determine cross-boundary access requirements?
Why do you need different types of trusts?
What are functional levels, and why do you need them?
What are the guidelines for restricting trust relationships?
What are the possible issues that can prevent networks from supporting trusts?
What are the possible access requirements and the associated recommended trust types?
If you are asked to design appropriate trust models, where should you start?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Designing Forest and Domain Trust Models (p. 6.22)

Designing Authentication in a Heterogeneous Network
In chapter 6 of the textbook, read lesson 2 (pp. 6.26-6.33) and then complete the associated hands-on practice at the end of lesson 2. Consider the following questions as you work through the lesson:

What are the necessary steps for designing authentication in a heterogeneous network?
What are the major network authentication protocols available in Windows Server 2003?
How can you find out which authentication protocols can be used by different operating systems?
What are some of the techniques necessary for strengthening authentication processes?
What are some of the common guidelines for designing authentication for a heterogeneous network?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Designing Authentication in a Heterogeneous Network (p. 6.35)

Establishing Account and Password Requirements for Information Security
In chapter 6 of the textbook, read lesson 3 (pp. 6.37-6.49) and then complete the associated hands-on practice at the end of lesson 3. Consider the following questions as you work through the lesson:

How can you establish account and password requirements for information security?
What are the minimum requirements of strong passwords and password policies?
What are the characteristics of the password policies available for Windows Server 2003-based networks?

What are the technical controls for password policies and their limitations?

What are some of the options for managing the need for multiple policies?

What are the critical elements of a strong password policy?

What should you consider if you were to design an account lockout policy?

What are some alternatives to password-based authentication that you can recommend?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Designing a Strong Password and Account Policy (p. 6.50)

Chapter 6 Additional Activities
Complete the following:

Case Scenario Exercise (p. 6.52)

Questions and Answers (p. 6.60)

Designing Secure Communications Between Networks

This topic is associated with chapter 7 ("Designing Secure Communications Between Networks") of the MCSA/MCSE Self-Paced Training Kit (Exam 70-298) textbook. This topic focuses on the skills necessary for designing security for communication between networks and designing security for communication with external organizations.

Resources

Selecting Protocols for Virtual Private Network (VPN) Access
In chapter 7 of the textbook, read lesson 1 (pp. 7.3-7.11) and then complete the associated hands-on practice at the end of lesson 1. Consider the following questions as you work through the lesson:
Why do you need to implement a Virtual Private Network (VPN) solution?

What are the types of VPNs that work with Windows Sever 2003?

What are the major characteristics of the VPN protocols that Windows Server 2003 can use?

How does IPSec provide security for communications, especially when using the IPSec tunnel mode?

On what basis do you make a decision in selecting a specific VPN protocol for a specific communication task?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Selecting VPN Protocols (p. 7.11)

**Designing VPN Connectivity**
In chapter 7 of the textbook, read lesson 2 (pp. 7.13-7.23) and then complete the associated hands-on practice at the end of lesson 2. Consider the following questions as you work through the lesson:

What is the rationale for designing client and server VPN configurations?

What are the network infrastructure requirements for VPNs?

How do you integrate VPN servers on networks?

In what ways can you provide firewall configuration information to administrators to support Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP)/IPSec VPNs?

How will you design secure VPN connectivity?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Designing a Remote Access Server VPN (p. 7.25)
Designing Demand-Dial Routing Between Private Networks
In chapter 7 of the textbook, read lesson 3 (pp. 7.27-7.33) and then complete the associated hands-on practice at the end of lesson 3. Consider the following questions as you work through the lesson:

Can you explain what site-to-site demand-dial routing is?

Can you design secure demand-dial routing?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Creating a Site-to-Site VPN (p. 7.37)

Designing Secure Communications With External Organizations
In chapter 7 of the textbook, read lesson 4 (pp. 7.44-7.46) and then complete the associated hands-on practice at the end of lesson 4. Consider the following questions as you work through the lesson:

What are some of the most commonly used methods for securing communications with external organizations?

How do you resolve trust issues if problems occur in this regard?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Determining Where Trust Relationships Are Necessary (p. 7.49)

Completing a Communication Design
In chapter 7 of the textbook, read lesson 5 (pp. 7.51-7.53) and then complete the associated hands-on practice at the end of lesson 5. Consider the following questions as you work through the lesson:
What is the exact process of designing secure communications?

How will you translate business needs into technical solutions?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Translating Business Requirements into Technical Solutions (p. 7.55)

Chapter 7 Additional Activities
Complete the following:

Case Scenario Exercise (p. 7.56)
Questions and Answers (p. 7.60)
Designing an Access Control Strategy for Data (Part II)

This section is a continuation of the previous instruction. As was indicated previously, this section provides an overview of the skills necessary in designing an access control strategy for data.

By understanding the fundamental concepts associated with designing access control for data, you will be able to design a logical authentication strategy, design secure communication between networks, design security by server role, and design access control for enterprise data.

**Topics**

**Designing Security by Server Roles**

This topic is associated with chapter 8 ("Designing Security by Server Role") of the MCSA/MCSE Self-Paced Training Kit (Exam 70-298) textbook. In this section, you will learn how to design a baseline security template for all systems and create a plan to modify baseline security templates according to role.

**Resources**

**Preparing an Infrastructure for Security by Server Role**
In chapter 8 of the textbook, read lesson 1 (pp. 8.3-8.11) and then complete the associated hands-on practice at the end of lesson 1. Consider the following questions as you work through the lesson:

- How do you design security by server roles?
- What is a security template, and why do you need to use a security template?
- Under what circumstances should you apply security templates to servers?
- What are some of the criteria to consider if you were to select an implementation process for implementing security by server role?
- How can you design the organizational unit (OU) infrastructure for server role security?

Complete the following hands-on practice before moving to the next lesson:

- Hands-On Exercise 1: Designing an OU Infrastructure That Can Be Used to Implement Security by Server Role (p. 8.12)
Defining a Baseline Security Template
In chapter 8 of the textbook, read lesson 2 (pp. 8.14-8.25) and then complete the associated hands-on practice at the end of lesson 2. Consider the following questions as you work through the lesson:

How do you find out which parts of a security policy can be applied to a baseline security template?

What is the rationale for interpreting an organization's security policy and applying parts of it to a baseline security template?

In what manner should you evaluate sample baseline security template recommendations?

How should you define a baseline security template for an organization?

What are some of the key elements of the security configuration that cannot be completed by using security templates?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Using a Security Policy to Define the Baseline Template (p. 8.26)

Designing Incremental Security Templates Based on Server Role
In chapter 8 of the textbook, read lesson 3 (p. 8.28) and then complete the associated hands-on practice at the end of lesson 3. Consider the following questions as you work through the lesson:

Under what circumstances should you group server roles?

How should you design an incremental security template?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Designing an Incremental Template for a Perimeter Network Server (p. 8.31)
Chapter 8 Additional Activities
Complete the following:

Case Scenario Exercises (p. 8.32)
Questions and Answers (p. 8.37)

Designing Access Control for Enterprise Data

This topic is associated with chapter 9 ("Designing Access Control for Enterprise Data") of the MCSA/MCSE Self-Paced Training Kit (Exam 70-298) textbook. This topic focuses on the skills necessary for designing an access control strategy for data, designing an access control strategy for directory services, analyzing auditing requirements, creating a delegation strategy, designing the appropriate group strategy for accessing resources, designing a permission structure for directory service objects, designing an access control strategy for files and folders, and designing an access control strategy for the registry.

Resources

Designing the Access Control Infrastructure
In chapter 9 of the textbook, read lesson 1 (pp. 9.3-9.23) and then complete the associated hands-on practice at the end of lesson 1. Consider the following questions as you work through the lesson:

How should you design control access to data in Windows Server 2003?
What are the proper ways to design an effective access control process?
How does permission inheritance affect access?
Where should permissions be stored?
How does inheritance affect the use of deny permissions?
What will be an accepted group strategy for accessing resources?
If you were to design a permission structure for files and folders, what would you do first?
What are some of the recommendations necessary for designing a permission structure for registry keys?
Complete the following hands-on practice before moving to the next lesson:

**Hands-On Exercise 1: Evaluating Permission Inheritance (p. 9.24)**

**Designing the Delegation and Permission Structure for Active Directory Objects**
In chapter 9 of the textbook, read lesson 2 (pp. 9.27-9.31) and then complete the associated hands-on practice at the end of lesson 2. Consider the following questions as you work through the lesson:

- What is the object permission structure for Active Directory used for?
- How can you design a delegation to distribute administration duties?
- What would you need to consider if you were to design the delegation structure for Active Directory?
- How should you design the object permission structure for Active Directory?

Complete the following hands-on practice before moving to the next lesson:

**Hands-On Exercise 1: Reviewing a Permission Structure Design (p. 9.34)**

**Analyzing Auditing Requirements**
In chapter 9 of the textbook, read lesson 3 (pp. 9.36-9.46) and then complete the associated hands-on practice at the end of lesson 3. Consider the following questions as you work through the lesson:

- What are the basic auditing requirements?
- Under what circumstances should you use Windows Server 2003 audit policies and system access control lists (SACLs)?
Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Determining What to Audit and Analyzing Audit Records (p. 9.47)

**Designing Security for Backup and Recovery Operations**
In chapter 9 of the textbook, read lesson 4 (pp. 9.54-9.58) and then complete the associated hands-on practice at the end of lesson 4. Consider the following questions as you work through the lesson:

What measures should you take to ensure that necessary cluster backup information and data are available?

Why is there a need to implement shadow copy?

Why do you need to design secure backup operations?

What would you do if you were to design security for backup and recovery operations?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Reviewing a Backup Plan (p. 9.59)

**Designing a File Encryption and Decryption Strategy**
In chapter 9 of the textbook, read lesson 5 (pp. 9.61-9.69) and then complete the associated hands-on practice at the end of lesson 5. Consider the following questions as you work through the lesson:

What should you do to ensure recovery of Encrypting File System (EFS) encrypted files?

Where should you start if you were to disable EFS?

What are the platform differences that affect the use of EFS?

What is the rationale behind the design of server-side storage for EFS?

What should you do if you were to design secure encryption and decryption of files?
Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Designing a Secure Encryption and Decryption Strategy (p. 9.71)

Chapter 9 Additional Activities
Complete the following:

Case Scenario Exercise (p. 9.72)

Questions and Answers (p. 9.77)
Creating the Physical Design for Client Infrastructure Security

This section provides an overview of the skills needed for creating the physical design for client infrastructure security.

Creating a physical design for a client infrastructure security system includes many facets of design. Designs include client authentication, security for client remote access, hardening client operating systems, and strategies for restricting user access to operating system features.

Topics

Designing a Secure Client Infrastructure

This topic is associated with chapter 10 ("Designing a Secure Client Infrastructure") of the MCSA/MCSE Self-Paced Training Kit (Exam 70-298) textbook. In this section, you will learn how to design a strategy for hardening client operating systems and how to design a strategy for restricting user access to operating system features.

Resources

Designing the Client Authentication Infrastructure

In chapter 10 of the textbook, read lesson 1 (pp. 10.3-10.16) and then complete the associated hands-on practice at the end of lesson 1. Consider the following questions as you work through the lesson:

What is the process necessary for designing a client authentication infrastructure?

What are the minimum authentication requirements?

How should you analyze authentication requirements for Windows clients?

Where should you start if you want to analyze authentication requirements for non-Windows clients?

Which methods can you use to analyze authentication requirements for communications with Internet Service Providers (ISPs) and mobile carriers?

Why do you need to establish account and password security requirements?

What is the proper way for you to design a client authentication infrastructure?

Complete the following hands-on practice before moving to the next lesson:
Hands-On Exercise 1: Designing a Client Authentication Infrastructure (p. 10.17)

**Designing a Secure Remote Access Strategy for Client Computers**
In chapter 10 of the textbook, read lesson 2 (pp. 10.18-10.42) and then complete the associated hands-on practice at the end of lesson 2. Consider the following questions as you work through the lesson:

- What is the recommended process for designing a secure remote access strategy for client computers?
- How should you design remote access policies?
- Which considerations should you take into account if you want to design access to internal resources?
- Why is there need for you to design authentication and accounting for remote network access by using Internet Authentication Service (IAS)?
- How can you use IAS to design an authentication and authorization strategy?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Designing a Remote Access Policy (p. 10.43)

**Chapter 10 Additional Activities**
Complete the following:

- Case Scenario Exercises (p. 10.45)
- Questions and Answers (p. 10.49)

**Designing a Secure Client System**
This topic is associated with chapter 11 ("Designing a Secure Client System") of the
MCSA/MCSE Self-Paced Training Kit (Exam 70-298) textbook. This topic focuses on the skills necessary for designing a strategy for hardening client operating systems and designing a strategy for restricting user access to operating system features.

**Resources**

**Designing a Strategy for Securing Client Computers**
In chapter 11 of the textbook, read lesson 1 (pp. 11.3-11.8) and then complete the associated hands-on practice at the end of lesson 1. Consider the following questions as you work through the lesson:

What are some of the typical techniques for designing a security for client computers?

What is the recommended approach in designing an organizational unit (OU) infrastructure for client computers?

Why do you need to implement an OU infrastructure for users, and what are the guidelines you should follow when designing it?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Designing an OU Infrastructure for Client Computers (p. 11.10)

**Designing a Strategy for Hardening Client Operating Systems**
In chapter 11 of the textbook, read lesson 2 (pp. 11.12-11.31) and then complete the associated hands-on practice at the end of lesson 2. Consider the following questions as you work through the lesson:

Where should you start if you want to design a strategy for hardening client operating systems?

How can you design effective security templates for basic operating system hardening?

How can you design administrative templates to manage application features?

Why do you need to implement the Internet Explorer Administration Kit (IEAK) in your network?

What is the recommended approach in designing software restriction policies to manage application use?

Do you know how to design the implementation of security structures?
Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Analyzing Administrative Template Settings to Control Application Features (p. 11.31)

**Designing a Strategy for Restricting User Access to Operating System Features**
In chapter 11 of the textbook, read lesson 3 (pp. 11.33-11.35) and then complete the associated hands-on practice at the end of lesson 3. Consider the following questions as you work through the lesson:

Why do you need to design and implement a strategy for restricting user access to operating system features?

What are the Windows groups that you can use to restrict user access to operating system features?

How should you use the administrative templates to restrict user access to operating system features?

Complete the following hands-on practice before moving to the next lesson:

Hands-On Exercise 1: Translating a Security Policy that Controls User Access to Operating System Features (p. 11.38)

**Chapter 11 Additional Activities**
Complete the following:

Case Scenario Exercise (p. 11.40)

Questions and Answers (p. 11.44)
Practice Test Review

Review all material using a practice exam format. The practice tests are supplied by ExamForce. Review the competencies you have learned and your readiness to take the MCSE Server 2003 Exam 70-298 (TSV2) assessment.

Topics

ExamForce

ExamForce has two parts: a testing engine and a database. It is a powerful tool because it is adaptive (i.e., it chooses questions from its database based on user weaknesses while still providing enough questions from strong areas to maintain strength). It divides what is presented into passes. Once you have completed three passes, you are ready to sit for the actual exam.

Resources

Learning Reinforcement and Review
ExamForce is a powerful tool; you will use it for review and final preparation. If you did not do so in the Preparing for Success section, you should now enroll for this resource through your AAP.

Take the ExamForce Pretest
This pretest will help you establish your baseline skill set. After you have taken the pretest, you will be able to determine your current level of proficiency. Please send the pretest results to your course mentor.

Work in Adaptive Drill Mode
In Adaptive Drill Mode, you will respond to a series of questions. The ExamForce interface includes a means for taking notes, which is handy as you respond. Incorrect answers will show a reference to the appropriate place in the included text. Also included is a historical analysis system to track and monitor your activities. In order to receive approval to take the assessment, you must successfully complete all three phases of assessment readiness in the historical analysis system, and you must e-mail your results to your course mentor for confirmation.
Congratulations

Upon completion of the practice exams, you will have successfully accomplished the goal of mastering the competencies set forth by WGU. By completing the chapters, lesson reviews, and hands-on practices associated with each competency, you have acquired the knowledge and skills necessary both for passing your TSV2 assessment and for gaining competence in and mastering Designing Security for a Microsoft Server 2003. If you feel that you are still not confident about the TSV2 assessment, please go over the competencies and their associated chapters before taking your TSV2 assessment.

Topics

Review of Competencies and Associated Chapters

As demonstrated above, this course of study covers four competencies of TSV2. Listed below are the four competencies and their associated chapters:

Competency 411.2.1: Prevention, Detection, Isolation, and Recovery
The graduate can design a framework for implementing security using prevention, detection, isolation, and recovery.

Chapter 2: Designing the Logical Infrastructure

Competency 411.2.2: Technical Constraints
The graduate can analyze technical constraints in designing security.

Chapter 1: Creating a Conceptual Design for Network Infrastructure Security
Chapter 12: Designing Security for Wireless Networks
Chapter 13: Designing Security for IIS

Competency 411.2.3: Access Control Strategy
The graduate can design an access control strategy for data.

Chapter 6: Designing a Logical Authentication Strategy
Chapter 7: Designing Secure Communications Between Networks
Transfer/Application to Work

Acquiring knowledge from textbooks is only part of the learning process. The ultimate goal of learning is to turn knowledge into skills that can be readily applied in the practical field. The following are some recommendations for transferring knowledge acquired through textbooks into practical skills in a real work environment:

Emphasis on hands-on practices: Practice makes perfect. Hands-on practices help turn short-term memory into long-term memory. Finally, personal experiences also help reinforce learning outcomes.

Research solutions through various channels: There are many ways to research solutions on issues associated with planning and maintaining a Microsoft Windows Server 2003 network infrastructure. Since new issues may appear in the real work environment, textbooks are not broad enough to cover all issues. Learning through research helps explore new solutions to new problems.

Collaborate and cooperate with peers or other students: There are different ways of learning, including the use of cooperation and collaboration to facilitate learning processes. Working with your coworkers, fellow classmates, and even with other students on the message board will definitely exert a positive impact on your learning outcomes.

Next Steps: Take the Assessment
Once you have completed all the tasks associated with the competencies, chapters, activities, lesson reviews, hands-on practices, and pre-assessment(s), you can start scheduling for the actual assessment at a Prometric testing center.

Best wishes to you while taking the TSV2 assessment.

**Resources**

**Refer for the Assessment**

Note: Keep in mind that when you are searching for a testing site that Prometric is the default for this form. If you are going to a Pearson VUE center, you must state that in the notes areas so that you get the appropriate voucher. Once a voucher is sent, it cannot be replaced.

Log in to your MyWGU Student Portal.

Go to the "My AAP" tab.

In the list below "Course Details," find the assessment you would like to request.

In the "Assessment Scheduled Date" column, click "Schedule Now."

Rather than clicking "Search" in the window that pops up, complete a search using both of the following to find a testing site:


Enter at least the name and phone number of the Prometric or Pearson VUE site you have chosen. Note: If you will be using a Pearson VUE site, you must state that in the "Notes" field.

Once you have input the necessary information, click "Continue."

Enter three different dates and times. For third-party assessment requests, these dates are just placeholders and will not be used to schedule the exam. They have to be entered for you to request the assessment, however. Note: The dates must be at least two weeks from the day you request the assessment.

Click "Continue" once the dates and times are filled in.

If you need to take your exam at a Pearson VUE center, please enter that in the "Other Considerations" box that appears so that we can be sure to send you a Pearson VUE voucher. Note: Once a voucher is sent, it cannot be replaced. Click "Continue."

A request will be sent to your mentor for approval.

Note: Following your request, you will receive further instructions.
Report Your Score
Whether you pass the exam or not, you are responsible for getting the score report to WGU. Please also remember to include the score report cover sheet. It is found under the "Resources" tab of your AAP. To submit your score reports, you can do one of the following:

Scan the score report and e-mail it to scores@wgu.edu. (This is the preferred method. It generally takes up to 5-7 days.)

Fax it to 801-606-7021. (This may take longer than 5-7 business days for entry.)

Mail a hard copy to Western Governors University, ATTN: Assessment Delivery Department, 4001 S 700 E., Ste 700, Salt Lake City, UT 84107.

If you have any questions regarding this process, please ask your mentor for more information.

Feedback
If you wish to provide feedback on this course of study, please contact Cheryl Bagshaw at cbagshaw@wgu.edu.

Click here to review University ADA policy.