REVIEW LESSON

MTA Course: 98-367 Security Fundamentals
Lesson name: Understand Security Software
Topic: Understand Server Protection
(One 50-minute class period)
File name: SecurityFund_RL_4.3

Lesson Objective

4.3: Understand server protection. *This objective may include, but is not limited to:* separation of services, hardening, keeping servers updated, secure dynamic DNS updates, disabling unsecure authentication protocols, Read-Only Domain Controllers, separate management VLAN, Microsoft® Baseline Security Analyzer.

Instructor preparation activities

- Install Microsoft Baseline Security Analyzer

Resources, software, and additional files needed for this lesson

- SecurityFund_PPT_4.3
- Network Printer
- Microsoft Baseline Security Analyzer

Teaching Guide

Essential Vocabulary

DNS dynamic updates—enables DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur. This reduces the need for manual administration of zone records, especially for clients that frequently move or change locations and use DHCP to obtain an IP address.

Microsoft Baseline Security Analyzer (MBSA)—an easy-to-use tool designed for the IT professional that helps small- and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance.

read-only domain controller—a read-only domain controller (RODC) is a new type of domain controller in the Windows Server® 2008 operating system. With an RODC, organizations can easily deploy a domain controller in locations where physical security cannot be guaranteed. An RODC hosts read-only partitions of the Active Directory® Domain Services (AD DS) database

network segmentation—the physical isolation of network traffic that flows between communicating systems. It is performed by a network device such as switch or router. As a result of network segmentation, the physical network is divided into distinct parts (segments) such as subnets (performed by a router) or VLANs (switch).

Windows Server Update Services (WSUS)—enables information technology administrators to deploy the latest Microsoft product updates to computers that are running the Windows® operating system. By using WSUS, administrators can fully manage the distribution of updates that are released through Microsoft Update to computers in their network.

Lesson Sequence

Activating prior knowledge/lesson staging (Anticipatory Set: 10 minutes)

1. Show the video on PowerPoint® slide 3: Introducing the Security Compliance Toolkit Series (Part 1 of 3).
2. What is included in the security guide? Give students a few minutes to respond.
3. As time permits, call on a few students to report to the group.

Lesson activity (30 minutes)

1. Teacher Instruction
   - Use the included PowerPoint presentation to review "server hardening."
   - At the end of the slides, ask the students to check if the "security goals" have been achieved on their computer.
   - Have each student share his/her answers with the whole group.
2. Guided Practice
   - Students experiment with the "Microsoft Baseline Security Analyzer".
   - Give students a few minutes to install, run, and print their findings. Allow them to work until they have finished..
   - As time permits, call on a few students to report to the group with their responses.

Assessment/lesson reflection (10 minutes)

Show the video *Security Baselines and Compliance Demo* (Part 3 of 3) (*http://mschnlnine.vo.llnwd.net/d1/edge/7/0/5/2/SCMBaselinesdemo_2MB_edge.wmv*)

1. On the same paper they used for the Anticipatory Set, tell students to summarize what they learned.
   - Be sure to give ample time for students to write their summaries.
   - If time allows, pick a few students to read their summaries.
2. At the bottom of the page, tell students to write any questions they have or any topics about which they would like more assistance.
3. After class, look through the student responses and follow up with any student requiring additional help.

Microsoft resources and Web links

- **Microsoft Baseline Security Analyzer**
  http://technet.microsoft.com/en-us/security/cc184923.aspx
- **Microsoft Security Center: Microsoft Security Assessment Tool**
  http://technet.microsoft.com/en-us/security/cc185712.aspx
- **Microsoft TechNet: Baseline Server Hardening**
  http://technet.microsoft.com/en-us/library/cc526440.aspx
- **Microsoft TechNet: What is RDOC?**
  http://technet.microsoft.com/en-us/library/cc755058(WS.10).aspx
- **MS Security Solution Accelerators Introducing the Security Compliance Toolkit Series Security Baselines and Compliance Demo**
  http://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx