REVIEW LESSON

MTA Course: 98-367 Security Fundamentals
Lesson name: Understanding Operating System Security 2.4
Topic: Understand audit policies
(One 50-minute class period)
File name: SecurityFund_RL_2.4

Lesson Objective

2.4: Understand audit policies. *This objective may include but is not limited to:* types of auditing, what can be audited, enabling auditing, what to audit for specific reasons, where to save audit information, how to secure audit information.

Resources, software, and additional files needed for this lesson

- SecurityFund_PPT_2.4
- Windows Server® 2008 R2 or Windows® 7

Teaching Guide

Essential Vocabulary

auditing—the process an operating system uses to detect and record security-related events, such as an attempt to create, to access, or to delete objects such as files and directories. The records of such events are stored in a file known as a security log, whose contents are available only to those with the proper clearance.

audit policy—a policy that determines the security events to be reported to the network administrator.

audit trail—in reference to computing, a means of tracing all activities affecting a piece of information, such as a data record, from the time it is entered into a system to the time it is removed. An audit trail makes it possible to document, for example, who made changes to a particular record and when.

security log—a log, generated by a firewall or other security device, that lists events that could affect security, such as access attempts or commands, and the names of the users involved.

Lesson Sequence

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

1. Student prompt (see Microsoft® PowerPoint® slide 3): On a sheet of paper, list the different "categories of security events" in Windows Server 2008 or Windows 7.
2. Give students a few minutes to respond, allowing them to work until they have finished.
3. As time permits, call on a few students to report to the group with their responses.

Lesson activity (40 minutes)

1. Teacher Instruction (20 minutes)
   - Use PowerPoint slide 8 to review the Windows Server 2008 Active Directory® Auditing and FGPP PM audio interview.
   - At the end of the presentation, ask the students to discuss the presentation.
2. Guided Practice (20 minutes; see PowerPoint slide 10)
   - Students investigate the Security Log and Event Viewer and discuss the individual entries.
   - Students then specify the categories of events that they want to audit. The event categories that they select constitute the audit policy.
   - Create a formal audit policy for a small business using the selections you just made. Expand each entry to show justification.
   - If time allows, you may review all or part of the selections and discuss the student choices.

Assessment/lesson reflection (10 minutes)

1. On the same paper they used for the Anticipatory Set, tell students to summarize the importance of auditing (see PowerPoint slide 11).
   - 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

- **TechNet: Advanced Security Audit Policy Step-by-Step Guide**
  http://technet.microsoft.com/en-us/library/dd408940(WS.10).aspx
- **TechNet: Audit Policy**
  http://technet.microsoft.com/en-us/library/dd349800(WS.10).aspx
- **TechNet: Security Auditing**
  (*http://technet.microsoft.com/en-us/library/cc771395(WS.10*
- **TechNet: Windows Server 2008 Active Directory Auditing and FGPP PM Interview**
  http://edge.technet.com/Media/592/