REVIEW LESSON

MTA Course: 98-367 Security Fundamentals
Lesson name: User Authentication 2.1_A
Topic: Understand user authentication
(One 50-minute class period)
File name: SecurityFund_RL_2.1_A

Lesson Objective

2.1_A: Understand user authentication. *This objective may include but is not limited to:* multifactor; smart cards; RADIUS; public key infrastructure (PKI); understand the certificate chain; biometrics; Kerberos and time skew; using Run As to perform administrative tasks; password reset procedures.

Preparation Details

Resources, software, and additional files needed for this lesson

- SecurityFund_PPT_2.1_A
- SecurityFund_SA_2.1_A
- SecurityFund_SA_2.1_A_Key

Teaching Guide

Essential Vocabulary

authentication—the process of obtaining identification credentials such as name and password from a user and validating those credentials against some authority. If the credentials are valid, the entity that submitted the credentials is considered an authenticated identity.

Kerberos—a network authentication protocol developed by MIT. Kerberos authenticates the identity of users attempting to log on to a network and encrypts their communications through secret-key cryptography.

lightweight directory access protocol (LDAP)—a network protocol designed to work on TCP/IP stacks to extract information from a hierarchical directory such as X.500. This gives users a single tool to comb through data to find a particular piece of information, such as a user name, an e-mail address, a security certificate, or other contact information.

remote authentication dial-in user service (RADIUS)—a proposed Internet protocol in which an authentication server provides authorization and authentication information to a network server to which a user is attempting to link.

terminal access controller access control system (TACACS)—a network access technique in which users log into a single centralized server that contains a database of authorized accounts. After the access server authenticates the user, it forwards the login information to the data server requested by the user.

Lesson Sequence

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

1. On a sheet of paper, have the students list as many different authentication processes as they can think of.
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 the included PowerPoint® slideshow to review the different types of authentication.
     - Show the methods and give the students 1 minute to process the question, "Where would you use this method?"
     - Then give the students 2 minutes to discuss answers with a partner.
     - Finally, have each pair or group of students share their findings with the whole group.
     - Repeat for each additional method review.
2. Guided Practice (20 minutes; please see the corresponding slide in the PowerPoint file)
   Students complete the worksheet, reviewing the purpose of each topic.
   - If time allows, you may review all or part of the worksheet, discussing student responses to the questions.

Assessment/lesson reflection (10 minutes)

1. On the same paper they used for the Anticipatory Set, ask students to summarize the importance of user authentication
   - 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 down 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

- **Windows Server® 2008 R2 Active Directory**
  http://www.microsoft.com/windowsserver2008/en/us/ad-main.aspx
- **Kerberos: The Network Authentication Protocol**
  http://web.mit.edu/Kerberos/#what_is
- **Overview of Authentication and Authorization Technologies and Solution End States**
  http://technet.microsoft.com/en-us/library/bb463152.aspx