REVIEW LESSON

MTA Course: 98-367 Security Fundamentals
Lesson name: Understanding Operating System Security 2.3
Topic: Understand password policies
(One 50-minute class period)
File name: SecurityFund_RL_2.3

Lesson Objective

2.3: Understand password policies. *This objective may include but is not limited to:* password complexity, account lockout, password length, password history, time between password changes, enforce by using group policies, common attack methods.

Preparation Details

Resources, software, and additional files needed for this lesson

- SecurityFund_PPT_2.3
- Administrative Tools installed

Teaching Guide

Essential Vocabulary

account lockout—a security feature in Windows® XP and Windows Server® 2003 that locks a user account if a number of failed logon attempts occur within a specified amount of time, based on security policy lockout settings. Locked accounts cannot log on.

password attack—an attack on a computer or network in which a password is stolen and decrypted or is revealed by a password dictionary program. The compromised password opens the network to the hacker and may also be used to reveal additional network passwords

password shadowing—a security system in which an encrypted password is stored in a separate "shadow" file, and its place is taken by a token representing the password. Password shadowing is used as protection from password attacks.

password sniffing—a technique employed by hackers to capture passwords by intercepting data packets and searching them for passwords.

Lesson Sequence

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

1. Student prompt (see PowerPoint® slide 3): On a sheet of paper, ask students to list10 different passwords. Next, have students "rank" the passwords in order of strength and complexity.
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, see PowerPoint slide 12)
   - Using the Internet, tell students to research and answer the 3 Password Attack questions
   - Show the slide and give the students a few minutes to process the information and come up with answers.
   - Have each student share his or her answer with the whole group.
   - Repeat for each additional bullet point.
2. Guided Practice (20 minutes; see PowerPoint slide 14 regarding this assignment)
   - On a sheet of paper, ask the students to list the Local Security Policies are on the computer they are working on.
     - Begin by opening Administrative Tools
     - Click on Local Security Settings
     - Open Account Policies
     - Click on Password Policy
     - What does the Security Setting column report to you?
     - Should changes be made? Why?
   - If time allows, you may review all or part of the paper, discussing student responses to the questions.

Assessment/lesson reflection (10 minutes)

1. Use PowerPoint slide 15 to show the steps to develop a password policy.
2. At the end of the slideshow, ask the students to share with the class their own experiences in using/enforcing password policies.
3. Be sure to give ample time for students to write their summaries.

4. If time allows, pick a few students to read their summaries.
5. At the bottom of the page, tell students to write any questions they have or any topics about which they would like more assistance.
6. After class, look through the student responses and follow up with any students requiring additional help.

Microsoft® resources and Web links

- **Password Best Practices**
  (*http://technet.microsoft.com/en-us/library/cc784090(WS.10).aspx*
- **System Key Utility**
  http://technet.microsoft.com/en-us/library/cc783856(WS.10).aspx
- **TechNet: Enforcing Strong Password Usage Throughout Your Organization**
  http://technet.microsoft.com/en-us/library/cc875814.aspx