CSCI 530 Lab 5

Authorization
Date Assigned: 2/16/07
Date Due: 2/26/07

Overview

In this lab, students will get to view the different preset local security policies in Windows 2000. Students will view the default local security policy, then view different preset policies, and compare the policies between them.

Instructions

1. Starting up the Windows Virtual Machine
    a. Open up VMWare by going to Start → VMWare → VMWare Workstation
    b. Click on the Windows 2000 Professional line under the "Favorites" Panel on the Left-hand side.
    c. Under Commands, select "Start this Virtual Machine."
    d. Wait the lengthy process until the Linux virtual machine starts up. It will have completely started up when you get a prompt for a user name. If at any time, you need the cursor back at the main system, press the CTRL and ALT keys at the same time.
    e. Once the Windows virtual machine has started, enter *Administrator* as the username and *password* as the password.
2. Viewing the users & groups
    a. Go to Start → Settings → Control Panel
    b. Double click on Users & Groups
    c. Click on Add…
    d. Enter the username: *jdoe*
    e. Enter the password: *password*
    f. Click on Other for the group, and select *Users* from the drop-down menu.
    g. Write down what the difference is between the *Users* group and the *Power Users* group.
    h. Click Cancel to cancel this process
3. Viewing the default local security policy
    a. Go to Start → Settings → Control Panel
    b. Double click on Administrative Tools
    c. Double click on Local Security Policy
    d. On the left-hand side, you will see tabs that allow you to view different aspects of the security policy. On the right hand side, you will see the actual policy settings. You can Double click on any individual policy to view the current setting and change any setting
    e. Double Click on Account Policies on the left-hand side to expand this policy
    f. Click on the password policy line on the left-hand side

g. What is the minimum password length? What is the setting for complexity requirement?
h. Double click on Local Policies on the left-hand side
i. Click on User Rights Assignment on the left-hand side
j. Which groups are allowed to access the system from a network? Which group is allowed to manage auditing and security logs?
k. Click on Security Policy on the left-hand side
l. What is the setting for Unsigned driver installation behavior? What is the setting for Unsigned non-driver installation behavior?

4. Loading a different policy
   a. Click on Security Settings on the left-hand side (the root of the tree)
   b. From the menu (in the VM), Select Action → Import Policy…
   c. You will see a list of templates. You can search the internet for these template names to get a better idea of what they are intended to do. For now, select hisecws, for High Security Workstation.
   d. Go to Password Policy under Account Policies (see above).
   e. Under this set of policies, what is the minimum password length? What is the setting for complexity requirement?
   f. Go to the User Rights Assignment under Local Policies. Which groups are allowed to access the system from a network? Which group is allowed to manage auditing and security logs?
   g. Go to Security Policy under Local Policies. What is the setting for Unsigned driver installation behavior? What is the setting for Unsigned non-driver installation behavior?
   h. In order to have the policy take hold of the system, you must restart the virtual machine, by going to Start → Shutdown, and selecting Restart from the drop-down menu.

5. Cleaning up
   a. Go to Start → Shutdown, and select Shutdown on the virtual machine. The virtual machine is set to non-persistant, so that all the changes will not be saved once the virtual machine is turned off. DO NOT CHANGE THIS! KEEP THE VIRTUAL MACHINE AS NON-PERSISTANT

Assignment

Write down the answers to each question posed in the instructions. In addition, answer the following questions:

1. Why would the high-security workstation setting allow for non-driver installs to succeed?
2. Why would Windows 2000 come with a very non-secure default setting for the local policies? What is the trade-off for tightening security on a system by default?