CSCI 530 Lab 9

Vulnerability Assessment
Week Assigned: 11/6/2006 – 11/10/2006
Week Due: 11/13/2006 – 11/17/2006

Overview

In this lab, students will set up two virtual systems, one running the latest Phlak Linux Live CD, one running an unpatched version of Windows 2000. Students are going to test running Nessus, a vulnerability assessment tool, on the Windows 2000 machine.

Instructions

1. Start the Phlak Virtual Machine
    a. Click on the Phlak link on the left-hand pane.
    b. Click on Start this Virtual Machine.
    c. Wait a while until it loads up into the virtual machine.
2. Start the Windows 2000 Virtual Machine
    a. Click on the Windows 2000 link on the left-hand pane.
    b. Click on Start this Virtual machine.
3. Configure Nessusd
    a. Open up a root console by clicking on the root console button on the bottom pane (it's the second button from the left).
    b. Enter the command "nessus-mkcert". This creates the certification for logging into the nessus server.
    c. Hit enter for every prompt (default is perfectly fine for this lab), until you get back to the normal command prompt.
    d. Type in the command "nessus-adduser". This goes through the script for entering a new user for the nessus server.
        i. For the login, choose "root"
        ii. Hit enter for the certification (default).
        iii. For the password, choose "password" (you will have to enter it twice).
        iv. For the rules, simply hit CTRL-D to have no rules
        v. Hit "y" to confirm adding this user.
    e. Enter the command "nessusd –D" to start the nessus server. Note: You are running a fairly old version of Nessus. This is okay, since we are testing it against a fairly old O.S. (Windows 2000).
4. Start the Nessus Client
    a. ONLY PROCEED TO THESE STEPS WHEN YOUR LAB ASSISTANT HAS GIVEN YOU PERMISSION TO RUN THESE TESTS!!! IF YOU DO NOT FOLLOW THIS INSTRUCTION, YOU WILL KILL THE INTERNET CONNECTION IN THE LAB, AND YOU WILL NOT RECEIVE CREDIT FOR THIS LAB!!!
    b. Enter the command "nessus" to load the graphical nessus client.

c. Under the Nessusd host tab, enter "password" in the password box.
    i. Just use the default for the SSL Setup
    ii. Hit "yes" for accepting the certificate
d. You will automatically be brought to the "Plugins" tab.
    i. Check "Enable dependencies at runtime"
e. Now go to the "target" tab.
    i. Switch over to the Windows 2000 virtual machine
    ii. Open the command prompt by going to Start→Run, and enter "cmd" for the command.
    iii. Enter the command "ipconfig".
    iv. Copy the address that is stated in the IP Address line, and enter that address in the target box of the nessus window.
f. Hit "Start the scan"
g. You should see a box stating what system you are scanning, and what it is currently scanning.
h. Wait until the scan finishes, and it will give you a report. Do not stop the scan, even if it is going slowly.

5. View the Nessus report
    a. The report is broken down by subnet, and then by host. Click on the subnet, then on the host, and then you will see the report by port, and the severity. There are three types of alerts: notes, warnings, and holes. Holes should be repaired immediately, warnings are possible security problems, and notes are only things to be considered.
    b. View the report, and include any security holes that you might find. If you do not find any security holes, ask your lab assistant for help. You are scanning unpatched Windows 2000 systems: there should be holes ☺

Assignment

Include a brief description of any security holes that Nessus reported. In addition, answer the following questions:

1. We used Nessus through a Linux Live CD. What are the advantages and disadvantages to using Nessus in this manner?
2. We used the Phlax Live CD. Are there other live CDs that are specific for network security? What are they?
3. Nessus stated that it did not turn on certain high-risk scans. What are those scans (normally they are turned off in "safe-mode" scans)? When would you use them?