ICCM 2006 - Nessus

Note: For the lab, Nessus is already installed and registered, but no Nessus user has been added.

Lab Prep:

Installing and configuring Nessus:

This is already done

Download nessus rpm
Install nessus rpm
Register nessus
    When you download nessus you get the number, or any time you need one you can request one.
    /opt/nessus/bin/nessus-fetch --register XXXX-XXXX-XXXX-XXXX-XXXX
    The process of registering also downloads all plug-ins.
Add a nessus user
    /opt/nessus/sbin/nessus-add-first-user
Nessus rules (when you add Nessus users):
    accept|deny ipaddr/netmask
    accept|deny client_ip #client_ip is a special variable which is assigned at connect
    default accept|deny # The default rule must be the last rule in the set

The Nessus lab Preparation:

The Nessus Server

Open the Nessus server virtual PC (see notes at the end)
Log in as root on the Nessus server (Password: LightSys2006) and create the nessus user
    /opt/nessus/sbin/nessus-add-first-user root

Make sure Nessus is running
    Service nessusd restart

Determine what your IP address is and write it here: _____
    # ifconfig eth0

The Nessus Console:

Open the nessus client from on the Windows computer
Connect the client to the nessus server

The targets… Er. Clients

Open the virtual PCs

Windows:
    Log in as Administrator (password: LightSys2006)
    Start a cmd prompt
    Renew the IP address
        Ipconfig /renew
    Write down the new IP address here: _____
        Ipconfig

Fedora Core:
    Log in as root (password: LightSys2006)
    Renew the IP address
        # ifdown eth0; ifup eth0
    Write down the new IP address here: _____
        Ifconfig eth0
    Put an entry in /etc/hosts for the Nessus server

The Fun stuff – Scanning

Here are a number of scans to try:

1. Enable all the default options and scan the windows and Linux virtual PCs
2. Try enabling local scanning of the Linux and Windows servers and try scanning again
    - In Windows, create a user and give him administrator privs (Administrator account does not work)
    - Add that username and password to the smb credentials on Nessus
    - Create a diff between the two
    - In Linux, you can try using password level or key level security. We recommend key level.
3. Disable "safe checks" and try scanning them again.
    - Create a diff between the two

Using Virtual PC

Open Virtual PC through the start-menu -> programs -> virtual-PC

If the list of virtual PCs does not appear, you should see a CPU icon appear on the right side of the task-bar. Double-click this to get the list of PCs.

The computers in the lab are not capable of running all three virtual computer simultaneously. You will need to run the nessus pc at all times for this lab.

Start the Nessus PC by double-clicking it.

When it has started, click in the virtual PC to give it focus.
Press the right-alt key to regain control of your mouse.

The Accounts:

Windows user:	Administrator	Password: LightSys2006
Linux user:	root	Password: LightSys2006