CS 482: Selected Topics in Information Security
Spring 2005 – Section 1

Module 3 – Nessus Assignment

I. Nessus

Nessus is a powerful network analyzing tool that can be used by administrators to asses their network security level. There are two versions of Nessus currently available:

-Client-server architecture
-NeWT (for Windows)

In this session, we will focus on the client-server aspect of Nessus. In implementing the client-server architecture of Nessus, a Linux machine must act as the server, while the client can be either a Linux or a Windows host. Once you install the Nessus server on a Linux machine, you can install many clients at strategic points in the network. The Nessus server performs the actual testing while the client provides configuration and reporting functionality.

Deliverables

1- Install the Nessus server software (nessus-installer.sh) on the LinuxR1 machine in your network.

   Note: install the same software to run Nessus client on another Linux machine. Instead of starting the Nessus daemon with **nessusd –D** you type **nessus**

2- Install the Nessus Windows client software (NessusWX 1.4.5a) on WinXP-R1

3- Generate and **submit** a Nessus scan report on the 192.168.[n].96 /27 subnetwork

4- From the report you generated in step (4), identify one vulnerability from each level of the alerts (information, low level alert, and high level alert) and **submit** the following:

   - Explain each alert in detail, and find an exploit to use against that vulnerability. Explain and implement the selected exploit and then find, explain, and actually implement a fix for that vulnerability. Demonstrate the success of the fix by re-running Nessus and showing that the vulnerability is no longer reported.

Refer to the following links:

www.Nessus.org http://www.cert.org www.securityfocus.com

Reminder

Read Chapters 3-6 in the Operating System Security book for the test on the Thursday after Spring Break.