Derek Meyer
M.S.
Information Assurance
Major Professor: Tom Daniels

Xen Worlds Intrusion Detection Lab for CprE 531

Abstract:

The Xen Worlds environment was created as a frontend to launch and interact with multiple virtual machines (VMs) that an instructor builds on a host computer/server. Xen Worlds currently uses the KVM hypervisor to create a virtual environment for which instructors can host labs for students to remotely connect to and complete class assignments. One such lab is designed around and Intrusion Detection System (IDS) in which students can get experience configuring the IDS to capture malicious packets entering a network.

This lab will simulate some basic network traffic involving a web server and another server with Secure Shell (SSH) access enabled. A computer outside of the network will simulate the basic connections to the servers so the students will have to be precise with configuring the IDS so the legitimate traffic is not blocked. The lab also has an attack computer that is automated to attempt basic attacks on the web server and ssh server, and it is these attacks that students will be tasked to capture and block.

The following will further explain the steps required for an instructor to completely set up the IDS lab for the Xen Worlds environment on a server with a fresh installation of Red Hat Enterprise Linux 6 (RHEL 6).