5th Workshop on ICT Uses in Warfare and the Safeguarding of Peace (IWSP'13), Pretoria, 25-27 November

Developing a Virtualised Testbed Environment in Preparation for testing of Network Based Attacks

RP van Heerden, H Pieterse, ID Burke
DPSS, CSIR Pretoria, South Africa

B Irwin
Computer Science Rhodes University Grahamstown, South Arica

Abstract

Computer network attacks are difficult to simulate due to the damage they may cause to live networks and the complexity required simulating a useful network. We constructed a virtualised network within a vSphere ESXi environment which is able to simulate: thirty workstations, ten servers, three distinct network segments and the accompanying network traffic. The VSphere environment provided added benefits, such as the ability to pause, restart and snapshot virtual computers. These abilities enabled the authors to reset the simulation environment before each test and mitigated against the damage that an attack potentially inflicts on the test network. Without simulated network traffic, the virtualised network was too sterile. This resulted in any network event being a simple task to detect, making network traffic simulation a requirement for an event detection test bed. Five main kinds of traffic were simulated: Web browsing, File transfer, e-mail, version control and Intranet File traffic. The simulated traffic volumes were pseudo randomised to represent differing temporal patterns. By building a virtualised network with simulated traffic we were able to test IDS' and other network attack detection sensors in a much more realistic environment before moving it to a live network.