Paper for consideration, RAID 99

"Nidsbench - A Network Intrusion Detection System Test Suite"

Assessing IDS: Benchmarking techniques and technologies

Dug Song
Anzen Computing
p: (734) 669-0800
f: (734) 669-0404
514 East Washington
Ann Arbor, MI 48106

Dug Song is a Senior Engineer at Anzen Computing, where he focuses on intrusion detection system integration and security consulting. He has been involved in the deployment of enterprise-wide, distributed security solutions at several large government, corporate, and educational sites. Before joining Anzen, Dug was security administrator with the University of Michigan, where he authored the AFS/Kerberos support in SSH in the course of protecting a distributed computing environment with over 70,000 user accounts. Dug is also a regular contributor to the OpenBSD project.

Abstract

Nidsbench is a lightweight, portable toolkit for testing network intrusion detection systems. It implements the specific fault injection techniques outlined in Ptacek and Newsham's seminal paper on network intrusion detection evasion. It is designed for both real-time and automated use, and allows for the replay of arbitrary attacks or reference network data for comparative analysis.

This paper describes the design and implementation of our test suite, and our experimental evaluation of several popular network intrusion detection systems.

[Note: Sorry for the short abstract, but we are still in the process of determining the scope of our paper - we haven't finished procuring all the systems we wish to test, etc. We plan to have all of our research done well before July, however - may we send you a preliminary copy of our paper as an update once we write it? --dugsong]