Abstract

In this paper the authors discuss about HawkEye Solutions, a Network Intrusion Detection System (NIDS) that detects abnormal Internet Protocol (IP) packets. An Intrusion Detection System (IDS) is a computer-based information system designed to collect information about malicious activities in a set of targeted IT resources, analyze the information and respond according to some predefined security policy. An NIDS is a computer-based information
system designed to collect information about malicious activities in a set of targeted IT resources, analyze the information, and respond according to a predefined security policy. Authors here present the basic building blocks of the IDS that include mechanisms for carrying out TCP port scans, Traceroute scan, which in association with the ping scan can monitor network health. Finally the implementation of a Packet Sniffer provides generic level opportunity to detect various types of attacks, based on packet analyzing. The authors have also proposed and implemented a novel Expectation Maximization based intrusion detection algorithm called EMID. The implementation results in Matlab are presented and discussed. The authors endeavor to integrate EMID with HawkEye Solutions as a future work.

Reference

- Robin Hanson, Sterling Software, John Stutz "Bayesian Classification Theory" Technical Report FIA-90-12-7-01. Artificial Intelligence Research Branch NASA Ames Research Center, Mail Stop 244-17, Moffet Field, CA 94035, USA
- Pantos, “Packet Reading with libpcap”, April 2010 http://www.systhread.net/texts/200805lpcap1.php

Index Terms

Computer Science Wireless

Key words
Intrusion Detection System (IDS)
Intrusion Prevention System (IPS)

Host-based IDS
Network-based IDS
HawkEye Solutions
Expectation Maximization
Bayesian Classifier
EMID