A FRAMEWORK FOR INTRUSION DETECTION SYSTEMS EVALUATION

BANDARA L.R.J.

This dissertation was submitted to the Department of Computer Science and Engineering of the University of Moratuwa in partial fulfillment of the requirements for the Degree of MSc in Computer Science

Department of Computer Science and Engineering
University of Moratuwa
October / 2007

Declaration

I, Bandara L.R.J, confirm that this work submitted for assessment is my own and expressed in my own words and the work included in the dissertation in part or whole, has not been submitted for any other academic qualification at any institution.

Signature …….....

Date …….

Certified by (Supervisor):

Name …….....

Signature …….....

Date …….

Abstract

Information security plays a major role in today's IT enabled organizations. In this security stance, Intrusion Detection Systems (IDSes) is a very important element if not the most. Therefore it is very important to select the most suitable product to deploy in any organization concerned. In order to select the suitable IDS it is necessary to evaluate at least short listed number of products or it is necessary to rely on some third party organizations who evaluate these products. But only very few organizations are involving in evaluating IDSes and therefore the cost of hiring such an organization is very high and hence only a very few organizations can bear it where as small organizations have to depend of there own methods. Therefore it is essential for the research community to help in evaluating these products. But the research community can not rely on the methods used by the organizations that do the evaluations since those methods are proprietary and not publicly available.

This paper describes a method of using the existing freely available tools of generating a data set or a criterion/check list and a framework that can be used to evaluate intrusion detection systems for a specific facility using the proposed method of generating data set.

Finally we discuss the lessons learned using this kind of a framework to evaluate intrusion detection systems and the opportunities for further improvement of this framework and in this area.

The tool uses a check list or attack script list and a parser that passes parameters to an open source/free vulnerability scan engine according to the check list to attack the targets and then search the intrusion detection systems logs/database for any detection of those attacks. This will evaluate the quality of the signatures of the specific intrusion detection system. Then we use Snort IDS as the base line to benchmark other candidate IDSes (and possibly will try to benchmark at least one more IDS, as a proof-of-concept, due to the time limitation).

Acknowledgments

First of all I would like to thank my project supervisor Mr. Shantha Fernando. He is very supportive and is always there to help me. He guided me at every time when I was in trouble. And also I would like to thank the academic staff specially Dr. Sanath Jayasena who review our progress regularly throughout the year and who encourage us to meet the deadlines and guide us on the correct times for starting documentation etc., Dr. Gihan Dias and Mrs. Vishaka Nanayakkara who taught us how to do a literature review. And also I would like to thank the non-academic staff of the department who helps us in many ways during this study.

I would also like to thank Mr. Aruna B. Herath from SLT iDC for the help and guidance given from the starting until the completion of this research.

Finally I would like to thank my wife Saja for the patience, support, care and motivation from the starting of this postgraduate study. She also helped me converting Snort rules to Shoki manually and it needed huge amount of time and care.

Table of Contents

List of Figures

List of Tables