1 Introduction

Open Systems AG, based in Zurich and founded 7 years ago, is a company focusing on Internet Security. Besides security products and consulting services, Open Systems AG also offers managed firewalls, managed audits, and managed intrusion detection services. Consequently, Open Systems AG is very interested in new approaches to intrusion detection. Smart intrusion detection is one of them. Intrusion detection (ID) is the art of detecting inappropriate, incorrect, or anomalous activity on computer networks. Intrusion detection systems (IDS) which operate on a particular host to detect malicious activity on that host are called host-based IDS, and IDS that monitor and filter network data are called network-based IDS. Until today, very few large IDS have been implemented. Most of the time, one box is put to the outside of a firewall to protect a couple of important servers in a DMZ. They usually lack 24x7 monitoring and have the problematic property to generate a lot of false positive alerts. Too many alerts decrease the usability and the accuracy of an IDS. Consequently they are not taken seriously any more after a while since they are considered a waste of time. These false positives prevent IDS deployment to protect large scale networks. This flaw comes from the simplicity of today’s intrusion detection software. They are knowledge-based, very similar to anti-virus software. They usually read the network traffic and compare the flow of data to known attack patterns. Each time such a pattern is seen, an alert is generated. The problem is that today’s IDS are not sophisticated enough to really understand or at least provide the right information to manually verify if an attack was successful or not, or if there is suspicious follow-up activity showing that an attack has probably been successful.
2 Assignment

2.1 Objectives

The objective of this thesis is to extend the preliminary work done at Open Systems AG. The main problems are to determine what 'intelligent' features a smart intrusion detection system should have, to implement them, and to test them in a real life environment.

2.2 Tasks

- Get experience and become familiar with real life Intrusion Detection Systems. Recently published books discussing the subject are [Nor99, Amo99, MSK99, Ano99]. Get a feeling for how traditional IDS detect attacks and focus especially on the question why they report so many false alerts.

- Based on the experience acquired, develop a set of automated reactions that are able to decrease the number of false alerts. This can probably achieved by collecting additional information and by generating the right decisions out of them. Of course, the probability to detect an attack should not be reduced by the newly introduced measures.

- Develop, implement, and test a network-based smart intrusion detection system based on the theoretical results that were achieved during the previous phase. Compare its performance with existing IDS regarding the decrease in the number of false positives.

2.3 Deliverables

- At the end of the second week, a detailed time schedule of the diploma thesis must be given and discussed with the advisors.

- At half time of the diploma thesis, a short discussion of 15 minutes with the professor and the advisors will take place. The students have to talk about the major aspects of the ongoing work. At this point, the students should already have a preliminary version of the written report, including a table of contents. This preliminary version should be brought along to the short discussion.

- At the end of the diploma thesis, a presentation of 20 minutes must be given during the TIK or the communication systems group meeting. It should give an overview as well as the most important details of the work.

- The final report may be written in English or German. It must contain a summary written in both English and German, the assignment and the time schedule. Its structure should include an introduction, an analysis of related work, and a complete documentation of all used software tools. Three copies of the final report must be delivered to TIK.

References


